ISSN - 2067 3353
ISSN - 2393-1450
ISSN-L - 2393-1450

Appearing twice a year, the review aims to place debates in intelligence in an institutional framework and thus facilitate a common understanding and approach of the intelligence field at national and regional level.

The target audience ranges from students to professionals, from the general public to those directly involved in intelligence research and practice.

"MIHAI VITEAZUL"
NATIONAL INTELLIGENCE ACADEMY

National Institute for Intelligence Studies

20, Odăi Str.
Bucharest 1 - ROMANIA
Tel: 00 4037 7721 140
Fax: 00 4037 772 1125
e-mail: rrsi@sri.ro

www.animv.ro

Nr. 17-18/2017

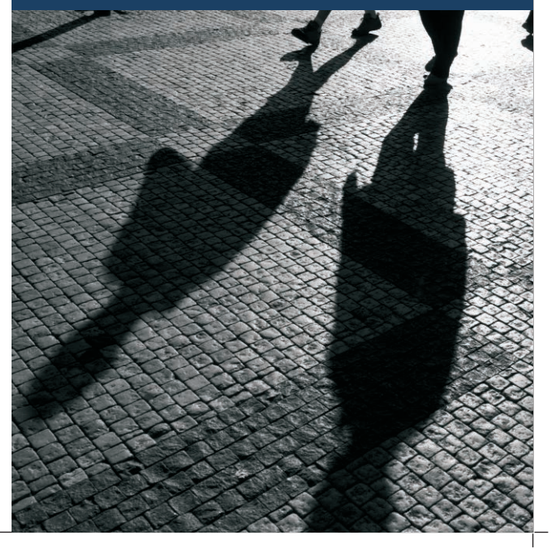
ROMANIAN INTELLIGENCE STUDIES REVIEW

National Institute for Intelligence Studies

RRSI Nr. 17-18/2017

REVISTA ROMÂNĂ de STUDII de INTELLIGENCE

ROMANIAN INTELLIGENCE STUDIES REVIEW



EDITURA ANIMV

"MIHAI VITEAZUL"
NATIONAL INTELLIGENCE ACADEMY

ROMANIAN INTELLIGENCE STUDIES REVIEW

Nr. 17-18/2017

This is the English version of the Romanian Intelligence Studies Review, an academic journal with scientific prestige, acknowledged by the National Council for the Validation of University Titles, Diplomas and Certificates (CNADTCU), indexed in the international databases CEEOL and EBSCO

Bucharest
2018

CONTENT

SECURITY PARADIGMS IN THE 21ST CENTURY

CONFLICT HIBRID, PROPAGANDĂ ŞI DEZINFORMARE – OBIECTIV STRATEGIC AL FEDERAŢIEI RUSE ÎN VECINĂTATEA APROPIATĂ ŞI ÎNDEPĂRTATĂ

Cristina IVAN *

Motto:

„Sovieticii au intuit cum funcţionează psihicul uman şi au folosit asta construind un scenariu simplu şi eficient: identifică motivele interne de conflict şi tensiune, denunţă aspectele divergente şi ambiguităţile care îşi fac loc în media, conferă-le semnificaţie şi repetă, repetă, repetă." (Thomas Boghardt, istoric militar şi de intelligence[1])

„La sfârşitul Războiului Rece, liberalismul şi-a croit drum spre est, către fostele state satelit ale Uniunii Sovietice. Douăzeci şi cinci de ani mai târziu, non-liberalismul de influenţă rusă îşi croieşte drum către vest prin sinuoasele coridoare ale instituţiilor democratice." (Conley, Mina, Stefanov, & Vladimirov, 2016, p. 5)

Influenţa regională a Federaţiei Ruse – între acumularea de capital strategic şi tranzacţionarea puterii simbolice

Rusia instrumentalizează informaţia ca armă într-un tip de conflict hibrid pe care îl poartă cu toate statele ce îi influenţează negativ capitalul de putere regională şi forţa de dominaţie asupra ţărilor pe care le consideră vecinătatea sa mai apropiată sau mai îndepărtată. Măsurile active ale Rusiei pun probleme nu numai statelor aflate în imediata sa apropiere, precum Ucraina, Moldova, Ţările Baltice, ci şi democraţiilor puternice central europene sau Statelor Unite ale Americii, care au ajuns să îi resimtă efectele nefaste în modul de influenţare a agendei politice, procesului electoral, sau în propagarea ideologiilor extremiste şi a polarizării sociale.

Metodele sale de operare sunt menite să producă confuzie, să distragă dezbaterea şi înţelegerea publicului de la aspectele cu adevărat importante ale agendei de politică internă, să erodeze suportul şi

* Cercetător Institutul Naţional de Studii de Intelligence.

[1] *Fingerprints of Russian Disinformation: From AIDS to Fake News*, New York Times, 12 decembrie 2017.

încrederea în valorile democraţiei şi în sistemul de securitate multilateral, bazat pe alianţe şi acorduri internaţionale. Unele state au răspuns proactiv la acest tip de ameninţare – Cehia, Slovacia, Finlanda –, altele s-au mulţumit să reacţioneze punctual sau deloc. Pentru a avea însă o imagine clară asupra **tiparelor acţionale şi a impactului mai larg european al măsurilor active întreprinse de Rusia,** propunem o scurtă trecere în revistă a ceea ce se cunoaşte despre modul de acţiune şi impactul ameninţărilor hibride în general, al propagandei şi dezinformării în mod special, pe teritoriul acelor state europene care s-au confruntat îndeaproape cu ea.

O privire transversală asupra regiunii central si est-europene demonstrează faptul că nu există o amprentă unică, care să poată fi determinată ca atare. Există însă un set de tehnici utilizate oportunist şi flexibil, în funcţie de vulnerabilităţile fiecărui stat în parte şi de oportunităţile deschise conjunctural. Există, în acelaşi timp, şi un mod de operare pe termen lung, ale cărui etape pot fi reliefate ca atare.

Tiparul acţional al ameninţării hibride, în accepţiunea şi modul de operare preferat de Rusia, este similar modului de incubare şi atac al unui virus. Heather Conley explică similitudinea astfel: strategia presupune **existenţa unei „faze de incubaţie",** identificată de unii autori cu perioada 2004-2008, în care măsurile informative au fost preponderent de natură clandestină şi au urmărit penetrarea aparatului de stat şi a unor sectoare economice considerate esenţiale: **sectorul energetic, sectorul financiar, media şi infrastructura din ţările ţintă**. Prin acest model se crează **o dependenţă structurală a sectoarelor economice cheie şi o reţea de patronaj facilitată prin corupţie şi trafic de influenţă**, care a slăbit coerenţa internă a statului ţintă şi care, în teorie cel puţin, poate ajunge până la capturarea totală a aparatului de decizie şi blocarea voinţei politice.

Î**n plan economic, influenţa rusă în ţările central şi est europene,** de exemplu, se poate observa, prin prezenţa corporaţiilor ruse pe piaţa internă, nivelul investiţiilor directe, nivelul tranzacţiilor comerciale, al proprietăţilor şi investiţiilor realizate de persoane fizice şi juridice având legături cu Rusia. Amplitudinea afacerilor ruse pe piaţa locală poate fi măsurată prin cifra de afaceri, bunurile fixe şi mobile, indicatorii de angajare a companiilor aparţinând unor cetăţeni ruşi sau controlate de aceştia. Procentajul din PIB raportat la acestea devine astfel un indicator relevant pentru prezenţa şi acţiunea intereselor ruse în statul ţintă. (Conley, Mina, Stefanov, & Vladimirov, 2016, p. XI).

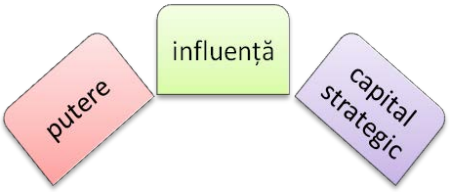
În studiul citat, realizat pentru perioada 2004-2014, de pildă, se face observaţia că orice stat care are o amprentă rusă care se ridică la

mai mult de 12% din PIB este semnificativ mai vulnerabil în fața influenței economice ruse și a a potențialului de capturare (Bulgaria, Serbia, Letonia), în timp ce în țările în care **amprenta nu depășește 12%, eforturile se îndreaptă în general către câștigarea unei influențe politice** prin care, eventual, să fie facilitată și penetrarea economică (Ungaria și Slovacia, perioada 2004-2014).

În faza a doua, gradual, se încearcă **compromiterea instituțiilor menite să combată corupția și practicile de monopol** (departamentele de combatere a corupției, ministerele de interne, procuratura etc.) (Conley, Mina, Stefanov, & Vladimirov, 2016). Odată blocată acțiunea acestor instituții, influența rusă se răspândește rapid.

În faza a treia, există două posibilități: capturarea aparatului de stat și avansarea intereselor ruse.

Sistemul democratic se dovedește rezilient și guvernul corupt este înlăturat. În acest caz, propaganda rusă intră în acțiune pentru a eroda și mai mult încrederea publicului țintă în autoritățile legitime, credibilitatea partidelor mainstream și a sistemului democratic în general, orientând potențialul de simpatie pentru partidele de extremă dreapta/stânga, anti-europene și anti-NATO.



FAZA 1	FAZA 2	FAZA 3
•penetrarea aparatului de stat •investiții în sectorul energetic, financiar, media și infrastructura din țările țintă •patronaj prin corupție, rețele de trafic de influență	•atacarea si compromiterea departamentelor de combatere a corupției, ministerelor de interne, procuraturii, serviciilor de securitate etc. •slabirea și uzura liderilor din sistemul de securitate	•capturarea statului •se continuă erodarea încrederii în autoritățile legitime, partidele mainstream și sistemul democratic •potențialul de simpatie este deturnat către partidele de extremă dreapta/stânga, anti-europene și anti-NATO.

Dezvoltarea rețelei de influență:

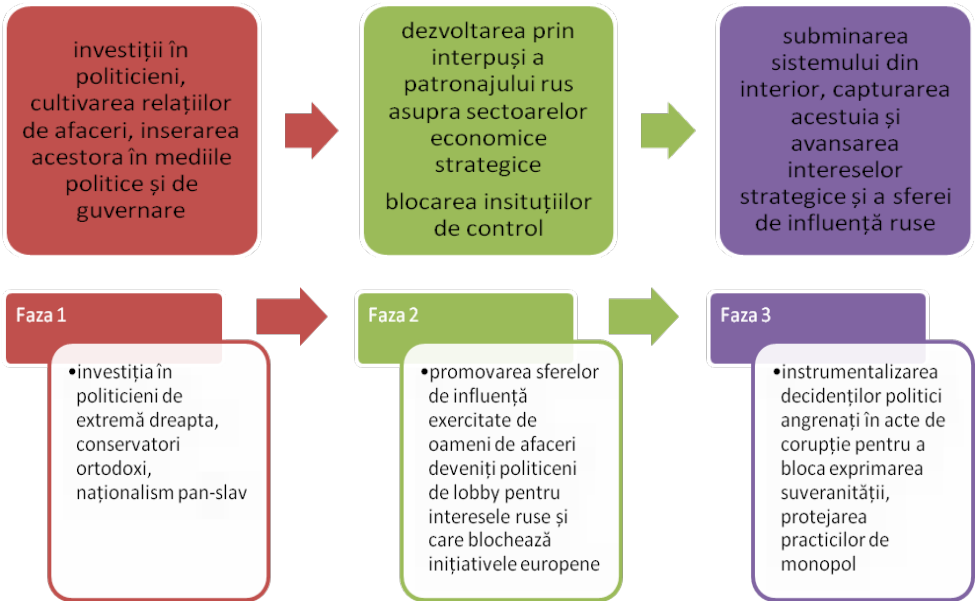


Figura 1: Capturarea statului – demers realizat de grupări de interese economice, militare, etnice sau de politicieni cleptocrați care au ca obiectiv influențarea treburilor statului în avantajul propriu prin mituirea șisau transmiterea de câștiguri ilicite, oneroase oficialilor în funcții și demnități publice (Conley, Mina, Stefanov, & Vladimirov, 2016, p. 1).

Măsuri de consolidare a proiecției de putere și prestigiu în plan regional și global

Una din temele predilecte ale propagandei ruse este reprezentată de proiecția capitalului de putere atât în plan intern, cât și în plan regional și global. Acest lucru se realizează, de pildă, prin construirea unui portret ideal al liderului, care să răspundă tiparelor de consum ale publicului țintă și care să fie suficient de versatil pentru a răspunde criteriilor de *entertainment* și prestigiu, promovate de industria cinematografică, de modă, aspirațiilor variate ale publicului țintă. Spre exemplu, imaginea președintelui Vladimir Putin ca „om universal" este realizată prin replici ale imaginii iconice holywoodiene - gentleman, sportiv de elită, vânător, pilot de avion, elicopter și rachetă, fashion-icon, tată de familie, protector al copiilor, iubitor de animale, agent 007. Sunt realizate și comercializate în acest scop calendare, obiecte de artă pop, de industrie vestimentară, parfumuri, suveniruri, se pun în scenă și

se imortalizează întâlniuri cu „miresele Moscovei". Toate aceste demersuri sunt de natură să îl transforme pe Putin într-un simbol al dezirabilităţii, al cărui surogat este obţinut prin achiziţionarea unor produse de consum şi al cărui capital de putere este astfel tranzacţionat nu numai în plan intern, ci şi în plan extern, în ţările învecinate, în care aceste produse se comercializează intens – de ex. pe litoralul Crimeei, în Bulgaria, Moldova etc. .

Emisiunile televizate sunt de asemenea consecvente în a creiona un portret al preşedintelui ca Eroul luptător pentru dreptate, valori umaniste şi creştine, prin opoziţie cu un întreg şir de lideri slabi şi corpuţi ale căror acte iresponsabile şi criminale pot produce haos şi dezordine. Un studiu realizat de Asociaţia Presei Independente în primăvara lui 2017, citat de Radio Europa Liberă, cu privire la emisiunile a cinci posturi de televiziune din Federaţia Rusă, arată care sunt temele predilecte de porpagandă puse în slujba formării şi menţinerii cultului de personalitate al preşedintelui Putin:

„În emisiunile informativ-analitice şi cele de autor difuzate la televiziunile monitorizate, şi anume Pervîi Kanal, RTR, NTV, REN TV şi STS, jurnaliştii promovează poziţia oficială a Kremlinului şi ideea că Vladimir Putin este unicul luptător împotriva terorismului şi apărătorul valorilor democratice şi al creştinităţii. Acelaşi mesaj este promovat chiar şi în buletinele de ştiri. Experţii notează că promotori ai acestuia sunt analişti, jurnalişti şi observatori care susţin ostentativ că UE ar degrada moral şi este pe cale de destrămare iar SUA şi NATO ar urmări doar scopuri de război." (Grejdeanu, 2017)

Proiecţia de legitimitate se continuă şi la nivelul populaţiei ţintă. Dacă UE este un organism agresiv care se pregăteşte să atace occidentul, are valori decăzute şi consumă alimente modificate genetic, Rusia este un spaţiu al valorilor şi bunurilor neatinse de poluarea globalizării. (Grejdeanu, 2017)

La nivel intern, proiecţia de putere în plan mediatic este completată de dezvoltarea unei reţele eficiente de tranzacţionare a capitalului material şi financiar şi crearea unui model distinct de regim politic şi economic care a primit titlul de *cleptocraţie (puterea hoţilor)*.[2] Karen Dawisha defineşte *cleptocraţia* ca un regim politic de tip mafiot, care acţionează prin intermediul unor reţele interconectate de asociaţii şi interese politice de clan centrate pe figura şi puterea simbolică a lui Putin şi care serveşte scopul de a consolida puterea acestuia, a reduce la tăcere vocile dizidente şi a maximiza beneficiile economice (Dawisha apud Conley, Mina, Stefanov, & Vladimirov, 2016, p. XII).

În acest tip de sistem, serviciile de securitate, autorităţile de stat şi organizaţiile de crimă organizată acţionează în mod conjugat pentru obţinerea capitalului financiar şi politic necesar perpetuării stării de fapt. **Influenţa rusă**

[2] Greaca veche Kleptes şi Kratos: kleptēs (hoţ) şi Cratus (Κράτος,putere), fiul lui Pallas şi Styx, reprezentare a forţei omeneşti şi puterii.

în plan extern a cunoscut gradual, în ultimii ani, o expansiune pe care în parte o datorează extinderii influenţei cleptocraţiei în ţările învecinate. Slăbirea sistemică, delegitimarea factorilor de decizie locali şi aproprierea resurselor financiare şi materiale în ţările vizate au avut, în subsidiar, şi acest tip de intervenţie ţintită pentru proiectarea sferei de influenţă. Capacitatea de a credita şi recompensa indivizii care se integrează în reţeaua cleptocratică devine astfel cheia de legătură pentru replicarea corupţiei în interiorul societăţii ţintă. Indivizii şi grupările astfel capturate vor servi în mod co-interesat interesele trasate de reţeaua cleptocratică.

Simultan extinderii reţelei cleptocratice de influenţă, propaganda rusă avansează în oglindă acuzaţii cu privire la astfel de practici derulate de serviciile secrete ale statelor inamice, acuzate de a avansa exact tipul de obiective şi practici pe care se sprijină puterea sistemului cleptocratic local.

Se încearcă astfel convingerea publicului ţintă, fie de faptul că adevărul este mult prea greu de aflat, fie de faptul că orice acuzaţie împotriva Rusiei face parte dintr-o schemă conspiraţionistă agresivă şi belicoasă. Unul din exemplele cele mai citate de literatura de specialitate este acuzaţia de doborâre a avionului AirMalaysia 17. TR a difuzat de pildă o ştire conform căreia un controlor de trafic numit Carlos ar fi postat pe Twitter că avioanele de vânătoare ucrainiene ar fi pornit în urmărirea respectivului zbor (Pomeranzev, 2016; Helmus, 2018). O altă ştire preluată de RT de pe un site conspiraţionist – Before It's News, citat de Helmus, punctează existenţa unui manual RAND adresat preşedintelui Poroshenko, prin care acesta "era învăţat" cum să conducă operaţiunea de reprimare a luptătorilor pentru libertate.

Alte zvonuri au avansat tema unui dezastru natural sau chiar apariţia inexplicabilă a unui batalion de luptă, din timpul celui de al doilea război mondial, care a doborât avionul în cauză. Evident, astfel de zvonuri circulate în media nu sunt neapărat menite să convingă audienţa, cât, mai ales, să producă neîncredere în posibilitatea de a afla adevărul (Qiu, 2017).

Mai recent, site-uri conspiraţioniste precum Milennium Project, care replică formatul Global Futures Forum prin crearea unei reţele de „oameni de ştiinţă" ruşi şi parteneri internaţionali[3] ce explică evoluţia mediului de securitate şi nu numai, se foloseşte de evenimente, crize şi tragedii curente pentru a ilustra ceea ce numeşte „acţiunile ilegale şi criminale ale principalilor adversari": state (de ex. Marea Britanie, care s-ar afla la originea manipulării

[3] Potrivit explicaţiilor furnizate într-o versiune mai veche a site-ului actual, Millennium Project este gestionat de Institutul Rus pentru Economie, Politică şi Lege şi Ministerul Industriilor, Ştiinţei şi Tehnologiei cu sediul la Moscova. Proiectul reuneşte o echipă interdisciplinară de cercetători ruşi şi cooperează cu institute de cercetare, universităţi şi ONG-uri din Federaţia Rusă, Europa, Japonia, SUA, China etc. (Sursa http://107.22.164.43/millennium/russia-02.html).

alegerilor americane), instituții internaționale (NATO), dar și țapi ispășitori vag identificați - statul american nevăzut (deep state), oculta mondială, Soros etc. .

Spre exemplu, incendiile devastatoare de pădure care au dus la distrugerea a trei orașe în proximitatea Atenei, din iulie 2018, sunt explicate, în chiar ziua dezastrului, de către site-ul conspiraționist, ca fiind un exemplu ilustrativ de atac terorist sub steag strain (plastic intitulat Firegeddon). Site-ul invocă folosirea unor tehnologii avansate de geo-inginerie - incendiu provocat prin drone, incendiatori tereștri și arme cu direcționare de energie (directed energy weapons). În spatele atacului sunt acuzate a se afla forțele NATO care doresc blocarea intenției Greciei de a se opune, alături de Italia, voinței ocultei mondiale.[4]

Concluzii

Interferența Rusiei în diseminarea unor conținuturi specifice procesului de propagandă și dezinformare este astăzi un fapt de necontestat. Un studiu menționează faptul că doar 6 dintre site-urile despre care există dovezi că sunt sponsorizate de Rusia au diseminat conținut de 340 milioane de ori, ajungând la 19 milioane de utilizatori (Bradshaw & Howards, Why does Junk News Spread so Quickly across the Social Media? Algorythms, Advertising and Exposure in Public Life, 2018, p. 9). Mai mult, Facebook a recunoscut în septembrie 2017 că a vândut între iunie 2015 și mai 2017, 3.000 de anunțuri publicitare către agenți ruși care acționau în cadrul Agenției Ruse de Cercetare a Internetului - așa numita fabrică de trolli. Aceștia nu promovau mesaje direct legate de un anumit candidat, ci se focusau pe teme cu potențial de polarizare socială în societatea americană: rasism, drepturile homosexualilor, controlul armelor și imigrație (Shane & Goel, Fake Russian Facebook Accounts Bought $100,000 in Political Ads, 2017). Mai mult, un număr de 470 de conturi având legături cu Rusia au fost dovedite ca fiind folosite pentru ca indivizi cu identitate fictivă să posteze drept activiști americani. Acestea au fost închise după ce au promovat mesaje care incitau la ură (Shane & Isaac, Facebook to Turn Over Russian-Linked Ads to Congress, 2017).

Dincolo de intervențiile țintite prin utilizarea tehnologiei, susținute sau facilitate de companiile furnizoare de tehnologii avansate, trebuie adăugat faptul că impactul acestui tip de campanii de dezinformare mai este multiplicat și de un soi de polenizare încrucișată de ideologii și simpatii, un aspect care, de altfel, caracterizează societatea globală. Aderențele ideologice sau simpla ocurență a unor interese de moment comune (de ex. dorința de a denunța acte de corupție, de a promova cauze ecologice, de a susține

[4] Pentru detalii vezi: http://themillenniumreport.com/2018/07/greece-targeted-with-geoengineered-wildfire-terrorism-photos/.

drepturile unor minorităţi afectate de război, discriminare, boală etc.) vor conduce la coagularea unui grup de suporteri şi diseminatori de mesaj din rândul unor categorii sociale şi culturale care, altfel, nu ar susţine obiectivele unei campanii de dezinformare: sub-culturi online, grupări de tineri, comunităţi de hackeri, mişcări ultra-progresiste, lideri de opinie în mediul online etc. Astfel de situaţii constituie premisele unor tactici de destabilizare fără precedent în ţările europene.

Referinţe bibliografice:

1. Bradshaw, S., & Howards, P. N. (2018). *Chalenging Truth and Trust: A Global Inventory of Organised Social Media Manipulation.* Oxford Internet Institute. Preluat pe iulie 26, 2018, de pe http://comprop.oii.ox.ac.uk/research/cybertroops2018/

2. Bradshaw, S., & Howards, P. N. (2018). *Why does Junk News Spread so Quickly across the Social Media? Algorythms, Advertising and Exposure in Public Life.* Knight Foundation, Oxford University. Preluat de pe https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/142/original/Topos_KF_White-Paper_Howard_V1_ado.pdf

3. Conley, H. A., Mina, J., Stefanov, R., & Vladimirov, M. (2016). *The Kremlin Playbook, Understanding Russian Influence in Central and Eastern Europe.* Rowman Littlefield. Preluat pe iulie 24, 2018, de pe https://www.csis.org/analysis/kremlin-playbook

4. Grejdeanu, T. (2017, aprilie 28). *Propaganda rusă în Moldova. Cum funcţionează?* Preluat pe iulie 30, 2018, de pe Radio Europa Liberă: https://www.europalibera.org/a/propaganda-rusa-in-moldova/28457231.html

5. Helmus, B. R. (2018). *Russian Social Media Influence. Understanding Russian Porpaganda in Eastern Europe.* Rand Corporation.

6. Pomeranzev, E. L. (2016). *Winning the Infomation War. Techniques and Counter-Strategies to Russian Propaganda in Central and Eastern Europe.* Center for European Policy Analysis.

7. Qiu, L. (2017, December 12). Fingerprints of Russian Disinformation: From AIDS to Fake News. *The New York Times*. Preluat de pe https://www.nytimes.com/2017/12/12/us/politics/russian-disinformation-aids-fake-news.html

8. Shane, S., & Goel, V. (2017, Septembrie 6). Fake Russian Facebook Accounts Bought $100,000 in Political Ads. *The New York Times*. Preluat de pe https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html

9. Shane, S., & Isaac, M. (2017, septembrie 21). Facebook to Turn Over Russian-Linked Ads to Congress. *The New York Times*. Preluat de pe https://www.nytimes.com/2017/09/21/technology/facebook-russian-ads.html

REGIONAL INTELLIGENCE SHARING - INSTITUTION OF DIPLOMACY AND ORDER & SECURITY DILEMMA IN THE CONTEMPORARY INTERNATIONAL SOCIETY

Adriana SEAGLE*

Abstract

After 9/11, intelligence has become a valuable product for small and large states to share or trade for power and small benefits in the international system. The EU and NATO share a sort of interdependence in significant number of frenemies, security risks and missions. However, empirical evidence shows that despite common threats and enemies, some states engage in intelligence sharing to affect positive change and reduce uncertainty, while others calculate and withhold intelligence either from fears of being passed on, irrelevant or low priority threats, or underdeveloped strategies to shape the future outcomes. Since the sharing process is intermittent and resembles puzzles with bits and pieces, what strategic value does the sale of intelligence have for the seller and the receiving state? To what extent does the sharing process enhance order and diplomacy versus alienation? Sharing intelligence is a practice of cooperation, but how is intelligence actually shared or sold, how much does it cost, what are the benefits of sale, and who bears the cost in the international society? These are interesting questions to explore on the role of intelligence in fostering international order and the contemporary security dilemma when engaging with the current transnational threats. This paper investigates whether regional intelligence sharing with the US enhances diplomacy and order in the European context or leads to possible security dilemma.

Keywords*: intelligence sharing, strategic value, cooperation, security dilemma.*

Introduction

In the intelligence sharing process, what is considered valuable information or valuable intelligence?[1] The era of new threats demands new

* Assistant Professor and Director of Intelligence and Security Studies (ISS), Bellevue University, USA, aseagle@bellevue.edu

[1] Information is not intelligence. Intelligence is the finished product resulted from the processed information that went through the intelligence cycle.

thinking, technologies and methods of intelligence collection and analysis, as well as new arrangements for intelligence sharing. Since 9/11, the world of intelligence is in continuous flux of transformation, adapting to "changes in the security environment, the political situations of various states, and the public pressures placed on the decision-makers to produce more population inclusion and security provisions."[2] As time progresses, the process of intelligence sharing seems to evolve and transform into an institutionalized norm of cooperation with rules and principles between small and large states. Theoretically, the intelligence sharing process is helping states define, understand and predict new threats and challenges within the international society. Practically, however, threats are multiplying, security budgets are increasing while fear and terror continue to invade the current security environment. Who determines the value of the information, how is intelligence transacted by states, and who benefits from intelligence transaction are procedural questions with important implications for academics and policymakers interested in assessing global security.

Although with the passing of time, states have increased intelligence sharing through the creation and implementation of various technologies and arrangements, when it comes to what is shared i.e. information or intelligence, the current literature does not provide an explicit understanding on the value of the information that is supposed to be shared or transacted with other states. Nor is there an explanation on what impact or value shared information has in the regional and global security context. Do states gather information for the pure sake of collection and sharing? In an era of proliferation of unknown threats and enemies, one may be tempted to say, "Yes!" Countries concerned with the amount of information collected, national security budgets and global security benefits question the purpose of information collection and sharing in context of producing sound policy. When pressed to assess the role of New Zeeland within the Five Eyes system, the Internal Affairs Minister, Peter Dunne underscored:

> *If we're collecting all this stuff holus bolus, the first question is why.* If the answer is 'because that's what Five Eyes says we should do and we simply hand it over to somebody else… that should be a proposition the (Intelligence Security Committee) must want to give some consideration to whether or not that's what we want (my emphasis).[3]

---

[2] Olli J. Teirila, "Small State Intelligence Dilemmas: Struggling between Common Threat Perceptions and National Priorities," *International Journal of Intelligence and Counterintelligence*, March 2015, Vol. 28:215-235.

[3] David Fisher, "Dunne: Inquiry must look at spy practices," *The New Zealand Herald*. 7, March 2015.

The question on the value of information collected is important for academics, as well as states in the evaluation of return investment on the relationship between intelligence sharing process and the enhancement of global security. The purpose of this paper is to explore the concept of intelligence's strategic value in the sharing process and focus on when and how intelligence gets an assigned strategic value. Moreover, the analysis delves into how intelligence sharing is an institution of order and diplomacy, as well as a form of insecurity in the contemporary international society. The paper will proceed first with a discussion on the exchanging of valuable and non-valuable information. Then, will focus on how intelligence sharing creates order and security dilemma for small states. In closing, it will discuss how intelligence sharing creates norms with rules and principles that mimic a full-fledged institution of diplomacy.

Sharing Intelligence - Trading Reciprocally Valuable Information for Information and Intelligence

Opinions in the intelligence sharing literature are divided over the extent to what and how information is shared. Scholars argue that information is traded for other information in 'simple' or 'complex' frameworks that enhance cooperation, as well as increase a security dilemma for both small and large states.[4] Jennifer Sims suggests that states barter intelligence using various costs and benefits including intelligence and political support, military assistance, intelligence dependency, political fallout, deception and embarrassment. In her view, the bartering process creates a security dilemma (a false appearance of transactional symmetry) when one side of the arrangement gets less than they put in. "Over time," Sims argues, "true gains in the trading process should be assessed, especially when the amount of value gained from the intelligence transaction is not equal - when one is getting more value than one gives in an exchange, should be a red flag for the responsible intelligence manager," because this is an indication of intelligence dependency and a false appearance of symmetry (Sims 2006:198).

A military and security policy professional argues that states cannot be relevant in the intelligence sharing process if they have no meaningful information to offer.[5] Captain Olli J. Teirila suggests that, in order to get

[4] Jennifer Sims, "Foreign Intelligence Liaison: Devils, Deals, and Details," *International Journal of Intelligence and Counterintelligence,* August 2006, Vol. 19, Issue 2, pp.195-217.

[5] Olli J. Teirila, "Small State Intelligence Dilemmas: Struggling between Common Threat Perceptions and National Priorities," *International Journal of Intelligence and Counterintelligence*. March 2015, Vol. 28:215-235.

prominence within the intelligence sharing framework, smaller states such as Finland "should have information to exchange with other countries' intelligence services in order to get something in return for itself" (Teirila 2015:228). Colin Murray claims that, even in context of special agreements such as the Five Eyes, states share continuously relevant information, but a transactional dissymmetry arises when states refrain from sharing everything with every member of the agreement mainly because of levels of classification and states special interests.[6] Regarding states special interests, studies have uncovered that states engage in intelligence sharing for both individual and collective benefits.[7]

James Walsh argues that intelligence sharing is a form of hierarchical cooperation reflecting both, states who control the process, draft rules of compliances and practices, and subordinate states who conform to the hierarchy in exchange for various benefits including "shared intelligence, foreign aid and military protection from external threats"(Walsh 2010:5). In light of these asymmetric transactions, some intelligence practitioners seem to suggest that despite costs and subcontracted intelligence collection agreements based on barter and hierarchy, states will still benefit from the sharing process even if they do not get immediately anything in return.[8] For example, a small state with an opportunity to reach other states or international organizations such as NATO or the IMF with information, and then having them follow that information with policies, in the world of intelligence, that will be considered a big gain.[9] In the intelligence sharing process, what is then considered valuable and non-valuable information and who determines the value of the information? For example, within the Five Eyes Framework, the United Kingdom may decide to share information on how many people use social media inside the UK. This information may be very valuable for member states interested in social networking, personal profiles, and so on but, may have no or less value for countries outside the Framework. Thus, context and threats characteristics have capacity to influence the value of the shared information.

---

[6] Colin Murray, "What the Manchester attack leaks mean for the UK-US intelligence-sharing relationship," *The Conservation Media Group*, 26 May 2017. Available at: https://theconversation.com/what-the-manchester-attack-leaks-mean-for-the-uk-us-intelligence-sharing-relationship-78415. Last Accessed on August 19, 2017.

[7] Adriana Seagle, "Intelligence Sharing Practices Within NATO: An English School Perspective," *Journal of Intelligence and Counterintelligence.* May 2015, Vol. 28: 557–577.

[8] Anonymous comment on the intelligence sharing process.

[9] Anonymous comment on the intelligence sharing process.

Scholars and practitioners alike suggest that valuable information comprises data that originates from a verifiable original source, and may be put to use or have potential to be used by the policy-makers. Jeffrey Richelson for example, assesses intelligence and its *value in relation to dissemination*. He claims that, "the greater the dissemination of the information, the greater the difficulty to judge the value of that information" (Richelson 1990:315).[10]This implies that in the world of intelligence, less valuable information is considered to be recycled information or information that comes from the second, third or more sources. Additionally, Irena Dumitru (2014:572) clarifies that valuable information is information collected on targets in which "the sources and methods of collection remain *unknown to the targets*" (my emphasis).[11] Cultural nuances and language skills capabilities seem to add value to the information at the beginning of the exchange. An emphasis on the veridicality of evidence indicates information coming from technology and human sources is considered, strategic, valuable and influences immediately a security protocol and/or policy. An example illustrating the trickle down approach of valuable intelligence is the incident of March 2017, when global media announced that the US banned electronics from the cabins of trans-Atlantic flights coming from the Middle East and North Africa citing "continuing threat to civil aviation."[12] The first valuable information regarding this incident has been exchanged several years earlier in 2014, when electronics were required to be screened separately and in some cases powered on to prove that they were real.[13]

> This morning, a new request to those traveling to the US, make sure electronic devices carried on board can power up. The fighting in Syria and now Iraq has alarmed American officials. Both countries have become a training ground for Jihadists, some from America and the west with a passport, which could allow easy access to flights. TSA is asking some of the 250 international airports with direct

[10] Jeffrey T. Richelson, "The Calculus of Intelligence Cooperation," *The International Journal of Intelligence and Counterintelligence*, 1990, Vol. 4, Issue 3, pp. 307-323.
[11] Irena Dumitru, "Building an Intelligence Culture From Within: The SRI and Romanian Society," *International Journal of Intelligence and Counterintelligence*, May 2014, Vol. 27:3, 569-589.
[12] Kaveh Waddell, "Abu Dhabi to Los Angeles: 17 Hours without a Laptop," *The Atlantic*. March 21, 2017.
[13] "New Airport Security Measures TSA Taking Closer Look at Electronics," *ABC News: Good Morning America*. July 7, 2014.

> flights to the US, to ask some passengers to power up cell phones, tablets, and computers. If that device doesn't power up, it won't go on the plane. Why? The worry is that bomb makers could be hiding explosives or components in those devices.[14]

When assessing the value and the impact a piece of information can have for a security policy one can assert that, in the contemporary period, big national and global security policy changes happen with very little notice, based on exchange of intermittent and small pieces of information that cannot be immediately or thoroughly verified. Also, despite long existing partnership, in the intelligence sharing process, small states may attempt to renegotiate how they transact valuable information with comparably larger states. An example of this complexity includes the media speculation that soon after taking office, the US president might have leaked information obtained from Israel to Russia. When pressed for an answer, former Israeli national security adviser, Uzi Arad lamented that in the sharing process, countries assume risks and benefits.

> Every nation considers many possibilities when sharing intelligence with another country, and that the more people they share with, the more their intelligence can be misdirected…the idea that the Trump Administration would share information with Russia that would find its way to Iran is a long shot…Russia could penetrate the US intelligence system using its own strong spying tactics…we also have rotten apples, others do too, *and you factor in [these considerations] when deciding to share intelligence, even with an ally* (emphasis mine).[15]

The Israeli official underscored the fact that small states participate in the intelligence sharing process consciously aware of the risk that the information they share may be compromised. The visit of the Russian delegation to the White House and the ensued dissensions over disclosing classified information to Sergey Lavrov is an illustration of compromising the intelligence sharing source, the methods of collection and the levels of classification. Pressed by media, the U.S. president disclosed that he shared

---

[14] "New Airport Security Measures TSA Taking Closer Look at Electronics," *ABC News: Good Morning America*. July 7, 2014.
[15] Yonah Jeremy Bob, Michael Wilner, "Trump won't leak Israeli intel to Russia, but Mossad might tread lightly," *The Jerusalem Post* online edition. February 6, 2017.

information with the Russian foreign minister due to concerns for humanity's safety and global security. "I wanted to share with Russia (at an openly scheduled W.H. meeting) which I have the absolute right to do, facts pertaining… to terrorism and airline flight safety ... plus I want Russia to greatly step up their fight against ISIS & terrorism," he tweeted.[16] According to a former U.S. official cited by the *Washington Post*, disclosure as such affected the future of the relationship with an intelligence sharing partner.

> President Trump revealed highly classified information to the Russian foreign minister and ambassador in a White House meeting last week. Trump's disclosures jeopardized a critical source of intelligence on the Islamic State.
>
> The information the president relayed had been provided by a U.S. partner through an intelligence-sharing arrangement considered so sensitive that *details have been withheld from allies and tightly restricted even within the U.S. government* (emphasis mine).[17]

Interestingly, after the oversharing incident, political officials and media have debated endlessly over the classification and ownership of the "code-word information," instead of focusing on the benefits of disclosing information for the preservation of individuals' safety; whose lives may have been spared from an unimaginable destruction. It is important to note that although in May 2017, the media continued to obsess over "safeguarding secrets" dilemma and disclosure of classified information, the information about the use of laptop computers on trans-Atlantic aircrafts appeared in open sources several months before it was publicly released, and had already influenced homeland and global security policies.

Who gains what from the disclosure or leak of intelligence? One may speculate that because of declassification, the U.S. actually saved money and took control over the message and the dissemination of information without asking a small country for permission. It is no secret that the U.S. is emphatically dedicated to collecting and classifying information. Annually, the U.S. spends billions of dollars to keep every *sneeze* and basic information secret. "It could be the name of a source, a method of collection that's still

---

[16] Demetri Sevastopulo, Katrina Manson in Washington, and Mark Odell in London,"Donald Trump defends sharing terrorism 'facts' with Russia," *The Financial Times*. May 16, 2017.
[17] Greg Miller and Greg Jaffe,"Trump revealed highly classified information to Russian foreign minister and ambassador," *The Washington Post*. May 15, 2017.

in use or an agreement with a foreign government that still needs to be protected" said John P. Fitzpatrick, head of the Information Security Oversight Office, which oversees the government's classification effort.[18] Another potential reason for disclosure may be to probe the validity of the existing information. There is no doubt that such information impacted financially the U.S. national security policy domestically, as well as internationally through intelligence and military operations in Syria and Iraq. In line of this argument, Sims also claims that states sometimes chose to reveal sources and methods of intelligence gathering in order to strengthen their influence (Sims 2006:197).

A challenge intrinsic to the asymmetry of information transactions pertains to the fact that global threats are relevant to the international community, yet not all members of that same community participate in implementation of information sharing policies or in generating initiatives to eradicate these same threats. For example, even though the self-declared Islamic *state* poses a common threat to the global community, some states seem to abstain from sharing pertinent security information with each other for fear of: (a) jeopardizing mutual trust, (b) revealing the information's source, (c) endangering ongoing cooperation with an ally, or (d) preventing the detection of "future" threats. As noted by the *Washington Post*, "the information released by the U.S., was so sensitive that it had not been shared with American allies and that circulation had also been tightly restricted within the U.S. government."[19] Is this an error of communication or a form of intelligence sharing politicization? Some speculate that, the U.S. president was not aware of the source of the information because he was just briefed on the issue, not on the source or the method by which it was obtained.[20] Yet, this indiscretion is illustrative not only of a "safeguarding secrets" dilemma, but also of a potentially severe fracture in the international community of intelligence transactions. Israeli officials refrained from making further comments reiterating the fact that Israel is not a member of the U.S. led coalition fighting the Islamic state, but is an active actor with enhanced

[18] Scott Shane, "Cost to Protect US Secrets Doubles to Over $ 11 Billion Dollars,"*The New York Times*. July 2, 2012.
[19] Cited by Demetri Sevastopulo, Katrina Manson in Washington, and Mark Odell in London, 'Donald Trump defends sharing terrorism 'facts' with Russia," *The Financial Times*. May 16, 2017.
[20] Oren Liberamann, "Israel may have to withhold intelligence from US, ex-Mossad boss Warns," *CNN Wire*. May 17, 2017.

capabilities of HUMINT and TECHINT who covertly shares info about threats with the U.S. and other coalition members.[21]

To complicate matters, the veridicality of information transactions comes under suspicion when information cannot be immediately verified and states use the opportunity to sabotage each other's political and economic interests by advancing their own interests. Then, leaks by accident occur to probe the veracity of the information in the public domain, control the message or let others know about the existence of certain information. Intentional and accidental leaks are also part of the intelligence sharing transaction process and may contribute to the information sharing dilemma. The news that the self-declared Islamic state acquired the capability to use sophisticated explosives in laptop computers on Middle Eastern airlines was met with skepticism by those affected who questioned whether the ban was in the name of security interests of the U.S., economic protectionism, or in the interest of some other actor interested in advancing a new piece of technology as a protective device of global security.[22]

Sharing Intelligence – The Strategic Value of Intelligence

When, in an intelligence security transaction, does information acquire strategic value for the seller and for the receiver? Some scholars suggest that a piece of information, acquires strategic value when for obtaining this information a country involves cost, technologies and countermeasures strategies.[23] The literature on the strategic value of intelligence is scarce. Yet, strategic value per se is a multidimensional concept linked to power, security and geopolitics. Likewise, some states are inclined to view the strategic value of intelligence in terms of maritime military capabilities and a balance of power.[24] By and large, the use of strategic intelligence in policymaking is intermittent, and some practitioners attribute this to the scarce production of strategic intelligence citing lack of expertise to produce it and disinterest of consumers to demand it. Others attribute the reorientation from strategic intelligence toward tactical and operational intelligence to limited

---

[21] Cited by Demetri Sevastopulo, Katrina Manson in Washington, and Mark Odell in London, "Donald Trump defends sharing terrorism 'facts' with Russia," *The Financial Times*. May 16, 2017.
[22] "Was Israel behind US laptop ban on Mideast airlines," *Al Jazeera English*. 17 May 2017.
[23] Griffith, Ivelaw L., "Caribbean geonarcotics.(Caribbean Security On The Eve Of The 21st Century)(narcotics traffic)', in *McNair Papers MNP, SS33*, Issue 52-55. 1 October 1996.
[24] Nazery Khalid, "With a Little Help from My Friends: Maritime Capacity-building Measures in the Straits of Malacca1," *Contemporary Southeast Asia ICSA 424*, Volume 31, Issue 3. December 1, 2009.

time available, the volatility of the security environment and the proliferation of risk.[25]

How does this impact national security policy? An informal survey of intelligence practitioners conducted by John Heidenrich reveals the convoluted meaning of strategic intelligence. "Hand someone a report on a foreign-related topic and describe it as "strategic intelligence" Heidenrich says, "and, then ask the recipient to explain the term "strategic intelligence" and how the report qualifies…a typical reply, after an awkward pause, has been that strategic intelligence is information about countries, or about nuclear forces, or perhaps a long-range forecast or…I don't know."[26] As Heidenrich defined it, strategic intelligence "pertains to strategy" and is "knowledge about obstacles and opportunities" obtained from multiple insights in the areas of politics, economics, engineering, language, history and culture.

It should prove interesting to learn via empirical studies when in the sharing process, the knowledge or information exchanged is labelled *knowledge of strategic value*. Hypothetically, some proponents of strategic intelligence may suggest that knowledge or information gets strategic value when it is used as a rationale for the creation and implementation of a strategy, such as "a grand strategy," or "a national security strategy." Some of these conceptions may come from experts in the fields of History, Political Science, Cultural Studies, Languages, World Religions, and so on. Still others may claim that lately the US Intelligence Community transacts more tactical (information for the battlefield) intelligence than strategic intelligence because of consumers' high demand of tactical intelligence and lack of expertise in areas dealing with religion, culture, history, corruption and civil affairs.[27]As indicated, strategic value of the information or intelligence can be linked not only to geopolitics, but also to intelligence cooperation and conflict resolution efforts. Essentially, information or intelligence seems to gain strategic value when states use it to influence policy development and implementation. Other scholars may also argue that

---

[25] George Cristian Maior, "Cunoasterea strategica in era globalizarii," in George Cristian Maior (editor), *Un Razboi al Mintii. Intelligence, servicii de informatii si cunoastere strategica in secolul XXI*. Bucuresti: Editura Rao, 2010, p. 46.

[26] John G. Heidenrich, "The State of Strategic Intelligence. The Intelligence Community's Neglect of Strategic Intelligence," *Studies in Intelligence*, Vol 51, No.2, 2007. Available Online. Last Accessed August 25, 2017.

[27] John G. Heidenrich, "The State of Strategic Intelligence. The Intelligence Community's Neglect of Strategic Intelligence," *Studies in Intelligence*, Vol 51, No.2, 2007. Available Online. Last Accessed on August 25, 2017.

even though after 9/11 the exchange of intelligence intensified, the quality of US security and foreign policy remains unaltered simply because policymakers are not eager to read or use strategic intelligence to inform policy development and implementation process.[28]

Intelligence Sharing - Small States and Security Dilemma

What is geographically a small state in the international society is not disputable. However, when considering the UK and Israel within the international community, the conception of a small state is less about geography and more about the power of its military and its intelligence capabilities to influence international relations. Doubtless, Europe is a collection of small states in geographical terms. What country gets the rank of "small" or "big" state in the intelligence sharing process is contingent upon the state's strength or capability to influence the sharing agreement and subsequently the international community through the amount and significance of information offered, as well as the frequency of transactions and the quality of the information at hand. Jonathan Alford comments on the security dilemma and the small states' ranking; and further argues that collecting, analysing and managing any amount of information and intelligence for the sake of procuring national security is difficult for small states because they have to invest in technology for collection, storage and analysis of germane information (Alford 1984:379). During the Cold War, some states boasted on their geographical advantage. Presently, however, geographical advantage of a small state is only an asset with potential for creating a security dilemma when a small state entrusts its own security or seeks security protection from great powers. Geographical position according to Alford, does not offer more than *a site* for a big power to project "a position of military advantage" somewhere else: "Great powers at war, will defend small states only if it is in their strategic interest to do so" (Alford 1984:381). How do states know what is in their strategic interest if policymakers do not use strategic intelligence to influence foreign policy decisions is a matter that requires further exploration.

During the recent NATO Summit, the US president delivered a speech which provides an insightful perspective into how great powers may respond to contemporary security challenges of small states when pressed by financial

[28] Marrin, Stephen, "Why strategic intelligence analysis has limited influence on American foreign policy," *Journal of Intelligence and National Security*, Vol. 32, Issue 6, 2017.

constraints at home. The theme of "America First" considered in the context of NATO's Article 5 concerned many NATO members since its first allusion in 2016, prompting the media to report headlines such as: "In NATO Speech, Trump is Vague about Mutual Defence Pledge," "Trump says US may not automatically defend NATO allies under attack," "Donald Trump Sets Conditions for Defending NATO Allies Against Attack," and "Trump finally commits to defend NATO allies."[29] A possible realist or Waltzian interpretation of the current situation within the international political system would imply that security is scarce and knowledge is expensive for states to share and to acquire. The American president announced publicly that NATO suffers from "chronic underpayment," even after states committed to allocate 2% payment in their latest agreements. The English School perspective on international relations and regional international society suggests small states ought to adopt a solidarist direction to enhance their common values and aspirations toward ensuring their own security within the creation of their own institutions, such as that of NATO.

Fairness in payment for collective security prompted NATO members such as Romania for example, to commit 2% of its GDP for national defence. Yet, some interpret this allocation toward small states' common security not as a reaction to the views from the US president, but rather a response to Russia's aggressive foreign policy. "We need a serious posture on deterrence, since Crimea is being militarized by Russia, and this can be used as a platform for power projection not only into the Black Sea, but to the south eastern Mediterranean," commented a NATO member.[30] In this current transactional environment, small states may have to re-examine and re-structure the nature and extent of their involvement with greater states. In like manner, small states may up their contributions to enhance their importance in relation to greater states and their strategic interests. Foremost, small states may consider the extent to which greater states may commit to their survival in case of military conflict.

---

[29] Michael D. Shear, Mark Landler and James Kanter, "In NATO Speech, Trump is Vague about Mutual Defense Pledge'. *The New York Times*. 25 May 2017. Justin McCurry. 2016. "Trump says US may not automatically defend NATO allies under Attack," *The Guardian*. July 21, 2016. David E. Sanger and Maggie Haberman, "Donald Trump Sets Conditions for Defending NATO Allies against Attack," *The New York Times*. July 20, 2016. Gregory Korte, "Trump finally commits to defend NATO allies," *USA Today*. June 9, 2017.

[30] Interview with Romania's Ambassador to the US, George Maior cited by Paul Mcleary, "NATO Spending, Romania Steps Up," *Foreign Policy*, May 3, 2017.

A careful review of transactional patterns of intelligence toward security within the international society reveals that the geographical size of the state does not matter as much as the behavior of the state and whether or not the state is democratic and relentless in pursuing common security interests. Predicaments for small states may arise from domestic weaknesses when setting up germane allocations within their budgets, strengthening democratic institutions, and preserving their social and political stability. Over a longer period of time, these weaknesses have the potential to erode and impact the strength of partnerships, and reciprocal trust from greater states. To complicate matters in this transactional framework, some authors indicate that small states may also be pressured by the international community or some of the greater states to release information that they are not ready to release. Other authors further attest that small states succeed by sheer persistence. For example, during and after the Cold War, Denmark managed to remain engaged in the intelligence transactional processes through "consistency, stubbornness, and expertise; earning the title of nuclear negotiator in Europe."[31]

Another predicament facing small states is recognizing and balancing both domestic and international developments and having logistical resources to deal with transactional issues. Olli J. Teirila mentions budget constraints and the proliferation of threats within the small states.[32] Using Finland as an example, Teirila discusses the domestic security predicaments some Eastern European states face between assuring high military budgets focused on collecting and sharing defence intelligence, as well as logistically being pressured to modernize national intelligence systems to keep up with domestic extremism and international society demands. A major contributor to small states security predicaments in Eastern Europe is the land grabbing threat coming from states with aggressive behaviour like Russia. As events continue to unfold within Russia, it is clear that the international society ought to focus more on the creation of the new norms and codes of conduct to regulate such menacing behaviour coming from greater states, like Russia. So far, this type of behaviour is enhancing the arms race for NATO member states, further having deleterious effects on flora and fauna through NATO's

---

[31] Vaidotas Urbelis, "The Relevance and Influence of Small State in NATO and the Common Foreign and Security Policy," *Lithuanian Annual Strategic Review*, 2014-2015, Vol. 13.

[32] Olli J. Teirila, "Small State Intelligence Dilemmas: Struggling between Common Threat Perceptions and National Priorities," *International Journal of Intelligence and Counterintelligence*. March 2015, Vol. 28:215-235.

deterrence and reassurance exercises. Foremost, this behaviour is disrupting the peaceful order of the international society.[33]

Diplomacy, Intelligence Sharing and Order Within Contemporary International Society

The post-Cold War world order as some rightly assess it, is in crisis with no specific norms to deal effectively with Russia's invasion of Crimea.[34] To contrast this threat, however, intelligence sharing transactional patterns evinces promise for a different type of enhanced cooperation among concerned states. But for this cooperation to be successful, it must be based on mutual trust and common security values by which participant states are commonly known friends and former enemies.[35] Hedley Bull writes about diplomacy and international order in a way in which "diplomacy includes both the formulation – gathering and assessing information on the international environment, and the execution of a state's foreign policy through cooperation, communication, persuasion and coercion"(Bull 1977:158). In his view, diplomacy is about tact and subtleties to minimize friction. Intelligence sharing-based transactions are a function of diplomacy toward equanimity: "while each country seeks to deny other countries some information about itself, it also wishes to impart some information" (Bull 1977:164). In the contemporary international society, the practice of intelligence-based transaction includes collection and sharing of strategic information not only about states, but also about groups and individuals through special envoys, special military attaches, journalists, and other representatives. All these entities provide constant flow of collection and sharing of strategic information.

---

[33] Jen Judson, "Building readiness: Romanian base gets an overhaul to strengthen NATO Forces,"*Defense News*. July 14, 2017. "Cutting a huge chunk of the hill-roughly 153 cubic yards of soil-in order to clear space for proper sightline between tanks on the range and the moving targets." "…a torrential volley of destruction…By the end of nearly an hour, the hillsides smoked from the unleashing of artillery, mortars, rockets and fire from tanks and combat vehicles as well as helicopters and fighter jets from Romania, the United States, Croatia, Armenia, Montenegro - the newest NATO member and Ukraine." Cited in Judson, "Multinational live-fire exercise lights up Romanian countryside in show of force," *Defense News*. July 18, 2017.

[34] Michael S. Kochin, "Transformations of World Orders: Lessons from Kissinger and the English School," Available online in *Academia.*

[35] Michael S. Kochin, "Transformations of World Orders: Lessons from Kissinger and the English School," Available online in *Academia.*

Based on Bull's definition of diplomacy, intelligence sharing is an essential feature of diplomacy and order within the international community. Intelligence sharing creates new norms of cooperation and mimics an institution of diplomacy within the international society. Intelligence sharing forges bilateral and multilateral diplomatic relations linking intelligence organizations within and between states not only according to states interests dictated by their resources and position within the international system as realists, such as Kenneth Waltz may suggest, but also according to states and organizations perceived security interests, values and opportunities, as the English School claims.[36] Intelligence organizations represent states not people, and in some intelligence sharing frameworks, relations are highly institutionalized through agreements and operate under mutually created and agreed upon rules and conventions (i.e., Five Eyes, NATO, EU, etc.). The institution of intelligence sharing is internationally recognized by states and is institutionalized through a web of operating centres or hubs which resemble state embassies dedicated to codification - cooperation of intelligence organization and intelligence organization under auspices of a director not an ambassador e.g., European Union's Intelligence Analysis Centre-INTCEN. The empirical tableau suggests also that, the intelligence sharing negotiation process may be both intermittent yet continuous; implies rules, framework agreements and allegiances to both the intelligence organizations and to the state.[37] Intelligence organizations have overlapping interests and the function of the intelligence sharing is to communicate information or intelligence within the international society and between one political community and another.

In retrospect, sharing intelligence or information exchange solidifies states relationships. A valuable piece of intelligence is collected and shared within the international society for the purpose of creating common rules or policies to preserve the society, its institutions and security. A piece of information becomes valuable when it is used immediately in policy to stop common threats to security. Value to the information is given first by actors who decide to collect, those who collect, process, and disseminate the information, as well as by the context and threats characteristics. Intelligence

---

[36] Kenneth Waltz, *Theory of International Politics*. New York: McGraw Hill. 1979.
[37] Mary Manjikian, "But My Hands Are Clean: The Ethics of Intelligence Sharing and the Problem of Complicity," *International Journal of Intelligence and Counterintelligence*, Vol 28, Issue 4, 2015. Stephane Lefebvre, "The Difficulties and Dilemmas of Intelligence Cooperation," *International Journal of Intelligence and Counterintelligence,* Vol. 16, Issue 4, pp. 527-542.

sharing can effect positive change within the international society. Further, withholding or intermittent release of intelligence due to concerns for protecting sources and methods of extrication, for example, may prevent the proliferation of some threats, but it may also disempower or alienate efforts for providing for global common security. Due to unpredictability and volatility of threats in the international security environment, the governing principle of intelligence sharing as an intrinsic feature of diplomacy ought to serve as a guiding principle for understanding threats and for preserving common security values and efforts by the international community to quench these same threats. This method may prove more advantageous than relying or endorsing secrecy of sources and methods for gathering strategic information.

References:

1. Alford, Jonathan, (1984), "Security Dilemmas of Small States," *The Round Table*, 292 (377-382).
2. Bull, Hedley, (1977), *The Anarchical Society, Third Edition*, Columbia University Press.
3. "Donald Trump defends sharing terrorism 'facts' with Russia," *The Financial Times*. May 16, 2017.
4. Dumitru, Irena, (2014), "Building an Intelligence Culture From Within: The SRI and Romanian Society," *International Journal of Intelligence and Counterintelligence*, May 2014, Vol. 27:3, 569-589.
5. Fisher, David, (2015), "Dunne: Inquiry must look at spy practices," *The New Zealand Herald*. 7, March.
6. Griffith, Ivelaw L., (1996), "Caribbean geonarcotics.(Caribbean Security On The Eve Of The 21st Century)(narcotics traffic)', in *McNair Papers MNP, SS33*, Issue 52-55. 1 October.
7. Heidenrich, John G., (2007), "The State of Strategic Intelligence. The Intelligence Community's Neglect of Strategic Intelligence," *Studies in Intelligence*, Vol 51, No.2.
8. Jeremy Bob, Yonah, Wilner, Michael, (2017), "Trump won't leak Israeli intel to Russia, but Mossad might tread lightly," *The Jerusalem Post* online edition. February 6, 2017.
9. Judson, Jen, (2017), "Building readiness: Romanian base gets an overhaul to strengthen NATO Forces,"*Defense News*. July 14, 2017, cited in Judson, "Multinational live-fire exercise lights up Romanian countryside in show of force," *Defense News*. July 18, 2017.
10. Khalid, Nazery, (2009), "With a Little Help from My Friends: Maritime Capacity-building Measures in the Straits of Malacca1," *Contemporary Southeast Asia ICSA 424*, Volume 31, Issue 3. December 1.

11. Kochin, Michael S., "Transformations of World Orders: Lessons from Kissinger and the English School," Available online in *Academia.*

12. Korte, Gregory, (2017), "Trump finally commits to defend NATO allies," *USA Today*. June 9.

13. Lefebvre, Stephane, (2003), "The Difficulties and Dilemmas of Intelligence Cooperation," *International Journal of Intelligence and Counterintelligence,* Vol. 16, Issue 4, pp. 527-542.

14. Liberamann, Oren, (2017), "Israel may have to withhold intelligence from US, ex-Mossad boss Warns," *CNN Wire*. May 17, 2017.

15. Maior, George Cristian, (2010), "Cunoasterea strategica in era globalizarii," in George Cristian Maior (editor), *Un Razboi al Mintii. Intelligence, servicii de informatii si cunoastere strategica in secolul XXI*. Bucuresti: Editura Rao, 2010, p. 46.

16. Manjikian, Mary, (2015), "But My Hands Are Clean: The Ethics of Intelligence Sharing and the Problem of Complicity," *International Journal of Intelligence and Counterintelligence*, Vol 28, Issue 4, 2015.

17. Marrin, Stephen, (2017), "Why strategic intelligence analysis has limited influence on American foreign policy," *Journal of Intelligence and National Security*, Vol. 32, Issue 6.

18. Mcleary, Paul, (2017), "NATO Spending, Romania Steps Up," *Foreign Policy*, May 3, 2017.

19. McCurry, Justin, (2016), "Trump says US may not automatically defend NATO allies underAttack," *The Guardian*. July 21.

20. Miller, Greg, Jaffe, Greg, (2017),"Trump revealed highly classified information to Russian foreign minister and ambassador," *The Washington Post*. May 15.

21. Murray, Colin, (2017), "What the Manchester attack leaks mean for the UK-US intelligence-sharing relationship," *The Conservation Media Group*, 26 May 2017. Available at: https://theconversation.com/what-the-manchester-attack-leaks-mean-for-the-uk-us-intelligence-sharing-relationship-78415.

22. "New Airport Security Measures TSA Taking Closer Look at Electronics," *ABC News: Good Morning America*. July 7, 2014.

23. Richelson, Jeffrey T., (1990), "The Calculus of Intelligence Cooperation," *The International Journal of Intelligence and Counterintelligence*, 1990, Vol. 4, Issue 3, pp. 307-323.

24. Sanger, David E., Haberman, Maggie, (2016), "Donald Trump Sets Conditions for Defending NATO Allies Against Attack," *The New York Times*. July 20.

25. Seagle, Adriana, (2015), "Intelligence Sharing Practices Within NATO: An English School Perspective," *Journal of Intelligence and Counterintelligence.* May 2015, Vol. 28: 557–577.

26. Sims, Jennifer, (2006), "Foreign Intelligence Liaison: Devils, Deals, and Details," *International Journal of Intelligence and Counterintelligence,* August, Vol. 19, Issue 2, pp.195-217.

27. Shane, Scott, (2012), "Cost to Protect US Secrets Doubles to Over $ 11 Billion Dollars,"*The New York Times*. July 2.

28. Shear, Michael D., Landler, Mark, Kanter, James, (2017), "In NATO Speech, Trump is Vague about Mutual Defence Pledge'. *The New York Times*. 25 May 2017.

29. Teirila, Olli J., (2015), "Small State Intelligence Dilemmas: Struggling between Common Threat Perceptions and National Priorities," *International Journal of Intelligence and Counterintelligence*, March 2015, Vol. 28:215-235.

30. Urbelis, Vaidotas, (2014-2025), "The Relevance and Influence of Small State in NATO and the Common Foreign and Security Policy," *Lithuanian Annual Strategic Review*, 2014-2015, Vol. 13.

31. Waddell, Kaveh, (2017), "Abu Dhabi to Los Angeles: 17 Hours Without a Laptop," *The Atlantic*. March 21, 2017.

32. Waltz, Kenneth, (1979), *Theory of International Politics*. New York: McGraw Hill.

33. Walsh, James I., (2010), *The International Politics of Intelligence Sharing*. New York: Columbia University Press. 2010.

34. "Was Israel behind US laptop ban on Mideast airlines," *Al Jazeera English*. 17 May 2017.

DEMOCRATISATION AND THE INTELLIGENCE SERVICE: A COMPARATIVE REFLECTION ON AFGHANISTAN AND ROMANIA

Diva PATANG*

Abstract

While Romania has been restructuring its intelligence service since the revolution in 1989, it has faced a number of obstacles and challenges to do with shaking-off former problems associated with the Securitate. Afghanistan has faced a similar challenge since the ISAF invasion of 2001 and has struggled with problems familiar to Romania, such as ethnic and sectarian factors; bureaucratic wrangles; and the continued influence of former communist actors and interests.

In Afghanistan, different political and religious stakeholders have led the reform of the intelligence service in opposite directions. Unlike the situation in Romania, the new NDS (National Directorate of Security of Afghanistan) lacks substantive reform and processes of legal and political oversight. While Romania seems to be moving in the right direction towards democratization and accountability, the same cannot be said of the security sector in Afghanistan, where intelligence operates in a controversial environment. On the jihadist threat, Romania has made progress, while Afghan intelligence is largely unable to counter the Taliban insurgency due to neighbouring countries. It seems that the key to success in Romania has been a move towards substantial democratization and demilitarization of the secret intelligence sector, and there may be much that Afghanistan could learn from this experience of transformation.

Keywords: *Afghanistan Intelligence, Romania Intelligence, NDS, Terrorism*

Introduction

The journey Romanian intelligence and security agencies commenced in 1948 now entered a determining juncture with the introduction of structural reforms to make intelligence relevant and fit it to the fight against terrorism and radicalization (Gheorghe, April 16, 2010). After the fall of the Soviet Union, Romanian security sector experienced mind-teasing and strenuous crisis when the country started professionalizing its law enforcement

* PhD Researcher, University of Buckingham, UK

agencies amidst ethnic and sectarian catastrophe and crunch in Eastern Europe (Gheorghe, April 16, 2010). At variance with, Afghanistan also experienced a critical period of foreign intervention and civil war during the cold war period, but no specific intelligence reforms were introduced (Gheorghe, April 16, 2010). In the 1980s, Afghan intelligence was at war, and 1990s, the whole intelligence infrastructure of the country disintegrated, and with the fall of Taliban regime, and intervention of the United States in 2001, Afghanistan recapitulated its journey, and established a new intelligence agency, National Directorate of Security (NDS).

The progressive and enlightened democratic objective of intelligence and Security Sector Reform (SSR) is to enable an efficient and well-organized delivery of security within a democratic structure (Royal United Service Institute (RUSI), 2009). Security Sector Reform is important for a war torn states like Afghanistan where the international community is struggling to reinvent state institutions by introducing smart Security Sector Reform packages (Friesendorf, February 2011). Intelligence and Security Reforms were particularly critical in Afghanistan, where warlords, war criminals, and insurgents groups are a major source of instability (United Nation Report, October 20, 2000). In a civil war, or in a traditional war between states, while state institutions are destroyed, the need for reinvention and reorganization is exceptionally important. After the fall of the Soviet Union in the 1990s, both Afghanistan and Romania resumed their democratic journey by restructuring the state and introducing Security Sector Reforms. However, Afghanistan once again embroiled in civil war after the Soviet withdrawal that caused the collapse of state institutions, while Romania continued its democratic journey after the Soviet withdrawal, and introduced intelligence reforms to build their state and strengthen the intelligence structure.

Afghanistan

Researcher and security expert, Mark Sedra has outlined the feature of Security Sector Reforms (SSR) in Afghanistan in her paper, and argued that donors have given inadequate attention to security sector in the war torn state: "The process to create a viable and effective security sector conforming to international standard is at the forefront of Afghanistan's state-building project. Known as Security Sector Reform, the process is viewed as the foundation on which progress in all other facets of the reconstruction efforts is dependent. However, in the Afghan context, it has been those traditional security mechanisms in the form of customary law, and militia systems, that

have remained intact, while modern formal structures nurtured through external assistance have shrugged to take form and acquire legitimacy" (Sedra, 2007).

Reforming intelligence in a newer democracy is extremely challenging process. Well established democracies, like USA or Great Britain, have developed institutions to deal with this dilemma, but balancing security with transparency is always a work-in-progress (Matei, 2011, p. 603). Achieving a balance between effectiveness and democratic control is an on-going challenge in any democracy. If older democracies can fail one way or another to balance democratic control with effectiveness, how can new democracies be expected to be successful? Currently, Afghanistan is lacking effectiveness and democracy as corruption and nepotism are causing trouble.

Moreover, the fundamental challenge of intelligence information gathering is the lack of coordination, reforms, and corruption in armed forces, police and intelligence agencies. The NDS, police commanders and army commander have been involved in several corruption cases during the last two decades. After 17 years of sustained operations, NATO and the US also failed to modernize and train Afghan intelligence, or force Afghan government to introduce Security Sector Reforms. Without understanding the cultural and social nature of information gathering in Afghanistan, Security Sector Reforms cannot be made effectively and successfully. Former US General Mr. Flynn in 2010 in his report had raised the same issue (Flynn, Pottinger, Batchelor, 2010). Security Sector Reform can be successful if the leadership believes that there is a need of reform. Obviously, political and economic institutions of a state must be stable in order for Security Sector Reform to be successful and endure over the long term. Absent this stability, Afghanistan with the assistance of NATO, will need to have programs in place to mitigate political and economic instability. Furthermore, Security Sector Reform must not become a quick fix solution, but rather it needs to be more carefully applied, in line with its original core tenets.

After the US invasion in Afghanistan, civil society and security experts expressed their reservations on the US and NATO inattention towards intelligence reforms and security equipment's. Almost certainly, the United States and NATO allies helped the NDS in making it fit to the fight against Taliban insurgents and other terrorist groups, but involvement of neighbouring states, put the security agency on ordeal. The agency needed more help in adorning its forces with modern technology, training and support, but civil society and experts often expressed reservation on this wool-gathering of international community. Illegal appointments and ethnicization factors are also agitating SSR.

Furthermore, in Afghanistan, different international, internal political and religious stakeholders, and private partners using intelligence service (NDS) for their political purposes. They want NDS to work for them and share intelligence with their circles (Jalalzai, 2017). Unlike the situation in Romania, NDS lacks legal and political oversight. NDS continues to suffer from key intelligence capabilities, especially in gathering intelligence information from remote areas to prevent neighbours' interference in Afghanistan affairs. While Romania seems to be moving in the right direction towards democratization and accountability, the same cannot be said of the security sector in Afghanistan, where intelligence operates in a controversial environment (Romania: OECD Public Governance Reviews, 2016).

Furthermore, NDS lacks reforms, legal, parliamentarian and political oversight, while in Romania, political, legal and democratic oversight is in place. In Afghanistan, intelligence operates in a controversial mood without leaders and professional approach to intelligence mechanism, while in Romania the current transformation and transition of intelligence are crucial for state security, with respect to democratization and effectiveness. On the other hand, Romania is struggling to democratize and professionalize its intelligence to counter jihadism, radicalization and international terrorism, while stakeholders within Afghan intelligence infrastructure resist reforms and organizational changes.

In addition, NDS is unable to adopt a professional approach to national security, while in terms of reorganization and reinvention process, in Romania control has been tightened around intelligence infrastructure through the creation of professional mechanism. This transformational and reorganizational process resulted in the creation of main intelligence agency (CNI) and provided an opportunity to the government to demilitarize secret agencies and empower the concept of the civilian infrastructure of intelligence.

Romania

With the fall of Soviet Union, Romania began reforming intelligence and security sector to consolidate democracy, and bring intelligence under democratic control to serve the community, but former communist intelligence infrastructure, internal and external stakeholder and bureaucratic culture occurred as an hindrance. These kinds of reforms painted a controversial image of the intelligence community in society (Davies and Gustafson, 2013), and it was notable considering the short amount of time for

the transition and foundations of the organisation – the Securitate (Matei, 2007, p. 629). The present picture is looking smart, but in reality, more work is needed to make intelligence relevant. Ethnic and bureaucratic stakeholders want their interests to be served, but notwithstanding these hindrances; Romanian media consecutively highlighted the importance of reforms and forced government to continue this process. At present, intelligence is facing severe criticism due to its inability to provide accurate information to the state and government institutions. Due to the lack of data, there are so many intelligence agencies in operation while the list of its membership is also unavailable. The law on national security, domestic and foreign intelligence, and law regarding the operational mechanism of intelligence address numerous challenges.

Furthermore, a new thinking of national security developed with the emergence of radicalization and extremism, ethnic and sectarian conflict that threatened the authority of weak states. Poland, Romania, Bosnia, and Bulgaria designed new counter terrorism strategies and introduced some immediate Security Sector Reforms to replace the communist intelligence infrastructure with a new competent security package. The war in Bosnia and Kosovo, fighting in Chechnya and its effects on Europe, sectarian and ethnic war between Armenia and Azerbaijan, and home grown extremism also forced the EU member state to introduce reforms and restructure their security infrastructure (Jayasundara-Smits and Schirch, 2016).

The significant challenge faced by Romania after the collapse of communism was how to deal with the legacy of its infamous Securitate-state intelligence agency. However, much of the challenge has been addressed during the Security Sector Reforms, while politicians, journalists, security experts, academics and Romanian officials stress the need to confront many obstacles to introduce reforms, and make intelligence professional and make it fit the fight against domestic extremism and international terrorism (Jayasundara-Smits and Schirch, 2016). A principle challenge for Romania was constraining its new intelligence apparatus to work within the boundaries of democracy while still being effective. Mechanisms of control and oversight were therefore created to balance the tension between security and liberty, and ensure that the intelligence agencies implement and observe the legal framework imposed upon them (Matei, 2007).

In the 1990s, the majority of Eastern European states began reforming their intelligence infrastructure to effectively respond to the exponentially growing threat of radicalization and international terrorism. Most intelligence studies in eastern democracies agreed on the importance of intelligence and

its role in the protection of state institutions. However, some recent research studies elucidate intelligence as a warning about looming threats, and also as an umbrella, a range of multifaceted activities including secret operations and planning (Shulsky and Schmitt, 2002). Romania and Afghanistan are different cases; in Romania, Security Sector Reforms have changed the culture of intelligence mechanism and collection, but the exponentially growing cases of corruption in state institution raised many questions including the transparency and fairness. While in Afghanistan, government and international community have concentrated on war strategies and operations, the intelligence and Security Sector Reforms process remained slow.

New forces emerged, and new intelligence units were established to tackle these new challenges. A movement towards more coherent intelligent state became the first priority of the EU member states while responding to a new kind of terrorism with a modern and democratic approach to national security. Having new security services, which people could trust rather than fear, and not fear of their own shadow, was what Romania wanted. While formal oversight mechanisms existed, informal control, mainly through the media, has been the primary oversight mechanism (Bruneau and Boraz, 2007; Matei, 2011, p. 219). Together, these developments led to a professional approach to national security and laid the foundation of structural reforms. The process of state building and reinvention of state institution faced some challenges, but with a relatively short space of time, this was tackled. These developments were perceived as successful scenarios of integration of different levels of policy and different epistemic communities.

The recent move against the culture of corruption and anti-government political developments in Romania raised irksome questions about the fairness of Security Sector Reforms process and democratic transformation. The issue of Security Sector Reforms and political transition in the country has been of great importance during the last two decades. Romania's problem with corruption became transparent while European Commission accepted its membership, but created natural selection, and oversight of Security Sector Reforms. On 18 January 2017, Intellinews reported the resignation of the deputy head of Romanian intelligence, Florian Coldea. Mr. Florian was forced to resign on 17 January 2017, while head of anti-corruption came under pressure to explain his position about the revelations of businessman Sebastian Ghita who claimed that security service was involved in shaping the DNA in partnership with the State Intelligence Agency (SRI) (Ernst, 2017).

Security picture in Romania presents entirely different shape. Romania is a peaceful state where reforms process is underway in a smooth way, but currently, its secret agencies came under media scrutiny, and have been criticized for a number of reasons, though much remains unclear due to a lack of accurate information. References to alleged misuse of the agencies by rival politicians are also all too common. According to Catalin Harnagea's argument; "Romania had (between 1996 and 2000) 12,000 active officers in the SRI alone, without mentioning anything about the other agencies" (Dragomir, 2011). Romanian officials often argue that clandestine personnel numbers are classified information valuable to national security. Drawing on testimony such as that of Harnagea, some critics have argued that the size of the intelligence service is disproportionate to Romania's actual security needs (Dragomir, 2011).

Analysis

If a state or a government wants to introduce Security Sector Reforms or wants to reinvent its law enforcement infrastructure, they need to change the mindset and bring about changes in persistent security structure. The case of Afghanistan and Romania is before us, which leads us to the bottom of a required argument. As we know, things are going in the right direction in Romania, but in Afghanistan, things are going in opposite direction (Dimitrakis, 2013). Afghanistan did not try hard enough to reinvent or reorganize its intelligence or introduce professional reforms to make NDS relevant. The country needs to build trust on intelligence agencies and their operations, but a recent political demonstration of the agency prompted deep criticism as the agency did not demonstrate in a right direction. The agency maintains its ethnic profile, spy on specific communities, and is, answerable to different political, religious and foreign stakeholders (Amnesty International, March 1991) One of the most criticised issues regarding intelligence services is the presence of former Intelligence officers in key positions within the government and intelligence agencies and the slow process of removing them from those services. It claimed theses ex-officers represents a roadblock to intelligence reform. How difficult is Afghanistan's reforms journey, and how ethnic and sectarian stakeholders create hindrances and trying to block intelligence and security reforms, these questions have been highlighted in Samim Arif's analysis: "Afghanistan's failure to bring reform to its security apparatus has been central to the continuation of unabated and enduring violence in the country. In 2016 alone, Afghan security forces lost more than 15,000 personnel in battle, and more than 16,000 Afghan civilians were killed.

At the leadership positions from the beginning of the new government, commanders have often integrated their ethnic militias into the Afghan National Army (ANA), Afghan National Police (ANP), and NDS. Even though there is a policy in place to represent all ethnicities proportionately, the criteria are fulfilled by the rank and file. Men lacking even high school degrees rose to the highest military ranks overnight" (Arif, 2017).

The main question Afghan civil society asks is that why NDS is weak, divided, and why NDS remains incompetent to respond to the exponentially growing terrorist attacks on civilian population. All components of Afghanistan's security sectors including, army, police and justice system, lack competency and professional mechanism. The police and army lack institutional leadership capacity, administrative and accountability system. The NDS failure in several districts occurs when an attack happens without warning (Jalalzai, 2014).

This agency (NDS), neither developed skills nor designed countering terrorism strategies during the last two decades. The NDS members are trained to collect intelligence information from remote areas, but the United States and its NATO allies still need to introduce intelligence reforms to make the NDS fit to the fight against radicalization and terrorism. The present infrastructure does not meet the requirements of counterinsurgency mechanism, as it is an irrefutable fact that secret agencies in Afghanistan have badly failed to obtain and gather information of significant worth which could otherwise prove to be in the best interest of its national security. NDS collect information from low-quality sources due to its undertrained intelligence personnel with limited access to advanced technology, such information gathered from the main cities and government departments can lead policymakers and military commanders to wrong conclusions.

Not with standing negative aspects of Romanian intelligence reform package and democratization process, there are positive things where new system of intelligence struggling to show a positive aspect of operational mechanism. The country's new intelligence infrastructure and its stakeholders are facing back-breaking and laborious resistance from old stakeholders who want to push the reform convoy of democratic forces to the brink. Reforms received mixed messages from civil society and intelligence experts. They say if intelligence agencies still maintain their command and control system within democratic system, or making influence government decision making process, at that point, the reform package cannot retrieve the support of citizens. On the ground, intelligence reform in the country has not been an easy task. Critics maintain that the culture of intelligence mechanism of the

communist era remains in place that make horses divert to a wrong way. The persisting complications in Romanian intelligence are corruption, stakeholdrism, and the operational mood of former Securitate agents. But, anyhow, the only way to make intelligence accountable and bring it under legal and democratic oversight is reforms.

These kinds of awkwardness also persisted in Afghanistan, but intelligence does not interfere in politics. Albeit, NDS has many negative points, but its constructive and efficacious aspects mechanism during the last 17 year war on terrorism cannot be disdained as the agency tried to counter insurgent forces by establishing countrywide intelligence networks. NDS lacks resources and intelligence information collection technology, but its fight against terrorism without a strong surveillance system and resources is of great importance. In 2017, NDS improved its operational mechanism, and gave the enemy tough time. Additionally, it identified the networks of Taliban and sectarian groups inside Pakistan.

On the jihadist threat, Romania has made substantial progress, and it seems that the key to success in Romania has been a move towards substantial democratization and demilitarization of the secret intelligence sector, and there may be much that Afghanistan could learn from this experience. On the other hand, Romanian intelligence agencies are under deep criticism for being under the political control of one man or one group. Bureaucratic control of intelligence operations, government and private stakeholders, and ethnic and sectarian factors are the most important aspects of Romanian intelligence infrastructure (Gheorghe, 2010). Afghanistan presents the same picture where foreign and domestic stakeholders control intelligence operations and create impediments against intelligence reforms.

In the case of Romania, notwithstanding the recruitment of civilians for intelligence agencies, the state intelligence still seems to be relatively closed to outsiders. The relationship between the President and army chief remains strained. Former communist elements within the intelligence agencies are creating trouble for policy makers and want to hijack intelligence and the reform package (Gheorghe, 2010). Correlated to Romanian intelligence, Afghan intelligence agencies are facing a similar crisis, where former communist and KGB trained officers controls intelligence and continue to spy on their opponents within the government and private sectors (Jalalzai, 2017).

The Romanian government has been endeavouring to consolidate a democratic culture of oversight, and strengthen reforms mechanism since 2000. In yesteryears, the old intelligence system was in operation with impunity and without democratic oversight, but in spite of all these

complicated operational mechanisms, intelligence was one of the most trusted state institutions, because awareness about the intelligence operation, oversight and its cooperation with law enforcement agencies were widely highlighted in print and electronic media. Having spotlighted factors featured to oversight and reforms, in 2008, Research Institute for European and American studies carried out a comprehensive study of the reform package of Romanian Security Sector Reforms: "The two factors can be credited with the transition of intelligence services; an aggressive media, which helped force the governments to democratic reforms. While formal oversight mechanism existed, informal control, mainly through the media, has sometimes been a more effective oversight mechanism to ensure that both the popular demand for democratic norms and the Western requirements for accession have been fulfilled. The media have exposed government wrongdoing to both domestic and international audience; thus, forcing the hand of the decision-makers to institute reforms" (Matei, 2008).

Similarly, media in Afghanistan is strong but unaware of the Security Sector Reforms or intelligence operations. Media always criticises or spotlights the weaknesses, political and sectarian affiliation of the members of Afghan intelligence agencies. However, intelligence reforms need to be addressed at the organizational level and the current mechanism used, needs to be restructured, while NATO and the United States have not taken this issue seriously. The relationship between intelligence agencies and electronic media is very peculiar; media wants to ensure agencies are accountable to civil society, while intelligence agencies want to operate in secret. These are two traditional ways of thinking, which contradict each other. Intelligence needs to operate secretly, to watch suspect, and arrest than to ensure the safety and security of citizens, while media want a front-page story.

Legal frame work to reshape the actions and operations of intelligence in Romania could not help authorities in bringing agencies under Democratic control in order to make effective intelligence, national defence supreme council exercised executive control over intelligence agencies. Intelligence information gathering in Romania is provided to every law enforcement agency. Constitutional principles protect personal data, and criminal procedural legislation allows intelligence gathering and surveillance (Born and Caparini, 2013). In 1990, Romanian President managed to establish Council of coordination and monitoring to ensure all activities of government relating to defence and state security; intelligence operations and national defence supreme council are performed in an organized form. The council is now watching and streamlining security operations and applies coordinative

strategies to make intelligence relevant (Law No. 39/1990). At variance with, after two decades of civil war, Afghanistan is still looking for a well-organized intelligence agency to defeat the Taliban insurgency, and other terrorist groups in order to ensure safety and security of its citizens. In May 2016, former President Karzai said: "The NDS job is to gather information and share it with other state institution, support policy makers, and parliament in legal issues."(Karzai, May 2016) When intelligence became an oppressive tool, then it needs to be reinvented through reforms. Due to its weak and controversial operational mechanism, NDS faces criticism from civil society and parliamentarians.

In Romania, Intelligence Service in its official report (2012) has defended its successful operations in various fields, and argues that political turmoil in the Middle East, Afghanistan, and Africa threatened internal security of the country: "In the Context of instability in Northern Africa and the Middle East, one of the most relevant developments in terms of security was represented by an increase in terrorist risks, meaning that the threat to Romania turned into a direct one, though in the absence an imminent terrorist attack (The Romanian Intelligence Service Report on the Activity, 2012).

When we read the reinvention and reorganization process of Romanian intelligence, reform package and oversight, we realize that the reforms and oversight aspect of the Romanian government is the best example of the professionalization of intelligence infrastructure for all European states. Numerous monologue, research reports, and books are available in EU, but the issue of intelligence reforms has received little attention of member states. This inattention resulted in the exponentially growing incident of terrorism and radicalization. Anyhow, Romanian intelligence is making things streamline to change the culture of communist era way of intelligence cooperation mechanism and introduce new strategies relating to counter terrorism approaches.

Conclusion

As there is limited information available to scholars and experts about the intelligence reform in Afghanistan, researchers are facing difficulties to spotlight negative and positive aspects of the NDS operational mechanism. The old communist infrastructure and way of intelligence information collections is still in place, hence, new and old system are in dissension. In yesteryears, Afghan governments informed civil society through various announcement and press releases that the process of intelligence reform was under way, but these announcements still remain on paper.

Over the past two decades, Romania tried to transform itself from an authoritarian state to a modern democratic state by introducing Security Sector Reforms which has not been easy. The Romanian government has made progress in resuscitating state institutions, and changing the communist culture of an intelligence operation, and information collection. Compared to other European states, Romania succeeded in implementing Security Sector Reforms, such as instituting effective democratic oversight over its law enforcement agencies. At variance, Afghanistan presents a different picture of lawlessness, civil war, corruption and warlordism that pushed the country to the brink.

These are harsh realities, and all these development on opposite direction in the country happened due to the lack of Security Sector Reforms, coordination, and professional security mechanism. If Afghanistan wants to overcome further decrepitude and disrepair and wants to make intelligence and law enforcement agencies competent, its leader can follow the lead of Romanian Security Sector Reforms or learn from the positive reform aspects of this country. The issue of Security Sector Reforms remained only on papers, while intelligence and law enforcement agencies are lacking professional mechanism and competent leadership.

NDS neither developed skills nor designed countering terrorism strategies during the last two decades. The United States and its NATO allies can support Afghanistan to introduce intelligence reforms to make the NDS fit the fight against radicalization and terrorism. In the case of executive and parliamentary control, how Afghanistan can apply some important principles of Romanian Security Sector Reforms, these reforms represent local culture, which cannot benefit NDS, or as every reform package and every state institution has its own political, cultural and economic background, therefore, Romanian reforms may not support the NDS operational mechanism, but in, generally speaking, these reforms can pave the way for Security Sector Reform in Afghanistan, as Afghan Intelligence agencies continue to suffer from key intelligence capabilities, especially in gathering intelligence information from remote areas. Afghanistan needs a legal framework to reshape its intelligence agencies and bring them under democratic control, but domestic and international stakeholders have set their priorities and strategies.

References:

1. *Amnesty International: Afghanistan: Reports of torture and long-term detention without trial*, March 1991.

2. Arif, Samim, (2017), *Security Sector Reform: Long Overdue in Afghanistan*, The Diplomat January 25.

3. Born, Hans, Caparini, Marina, (2013), *Democratic Control of Intelligence Services: Containing Rogue Elephants*, Ashgate Pub.

4. Bruneau, Thomas C., Boraz, Steven C. (2007), *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness*, 1st ed., Austin, Tex.: University of Texas Press.

5. Davies, Philip H. J., Gustafson, Kristian C., (2013), *Intelligence Elsewhere: Spies and Espionage Outside the Anglo-Sphere*, Washington, Georgetown University Press.

6. Dimitrakis, Panagiotis, (2013), *The Secret War in Afghanistan*, Library of Middle East History.

7. Dragomir, Elena, (2011), *The Romanian Secret Services, Politics and the Media: a Structural Overview*, on Balkanalysis.com, 20 April, http://www.balkanalysis.com/romania/2011/04/20/the-romanian-secret-services-politics-and-the-media-a-structural-overview.

8. Ernst, Julian, (2017*), Deputy Head of Romanian intelligence service resigns amid political scandal*, in "Intellines", 18 January, http://www.intellinews.com/deputy-head-of-romanian-intelligence-service-resigns-amid-political-scandal-113976/81.

9. Flynn, Michael T., Pottinger, Matt, Batchelor, Paul D., (January 2010), *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*, Centre for New American, http://online.wsj.com/public/resources/documents/AfghanistanMGFlynn_Jan2010.pdf.

10. Friesendorf, Cornelius, (2011), *Paramilitarization and Security Sector Reform: The Afghan National Police,* International Peacekeeping, Vol.18, No.1/ February 2011.

11. Gheorghe, Eliza Rodica, (2010) *The Romanian Intelligence Service during the Cold War*, thesis submitted to the Faculty of the Graduate School of Arts and Sciences of Georgetown University, B.A. Washington, DC, April 16, https://repository.library.georgetown.edu/bitstream/handle/10822/553496/gheorgheRodica.pdf.

12. Jalalzai, Musa Khan (2014), *Reforming Afghan intelligence agencies*, in Daily Times, 23 December.

13. Jalalzai, Musa Khan (2017), *The Afghan Intel Crisis*, Algora Publishing, New York.

14. Jayasundara-Smits, Shyamika, Schirch, Lisa, (2016) *EU and Security Sector Reform: Tilting at Windmill*, Global Partnership for the Prevention of Armed Conflict, 31 March.

15. Karzai, Hamid, (May 2016), *Interview,* London.

16. Law No. 39/1990 on the Setting Up, Organization and Functioning of the Supreme Council of National Defence, MO, Dec. 13, 1990, repealed by Law No.

415/2002 on the Organization and Functioning of the Supreme Council of National Defence, MO, July 10, 2002, https://www.sie.ro/legislatie_Legea_nr.415-2002.html (in Romanian), archived at https://perma.cc/GH7B-D2D4.

17. Matei, Florina Cristiana, (2007), *Romania's Intelligence Community: From an Instrument of Dictatorshp to Serving Democracy*, "International Journal of Intelligence and Counter Intelligence 20", no. 4.

18. Matei, Florina Cristiana, (2008), *Romania's Transition to Democracy: Press's Role in Intelligence Reforms*, Naval Postgraduate School USA, Research Institute for European and American Studies, Research Paper No-121, May.

19. Matei, Florina Cristiana, (2011), *Intelligence Reform in New Democracies: Factors Supporting or Arresting Progress*, The NPS Institutional Archive 18, no. 3 (Jun 2011).

20. *Romania: OECD Public Governance Reviews, the Centre of Government*, (2016), https://www.oecd.org/countries/romania/publicgovernance-review-scan-romania.pdf.

21. Royal United Service Institute (RUSI), (2009) *Reforming the Afghan National Police,* London, and Philadelphia: RUSI and Foreign Policy Research Institute.

22. Sedra, Mark, (2007) *Security Sector Reform in Afghanistan: An Instrument of the State-Building Projec*t, Part of the Palgrave Studies in Governance, Security, and Development book series (GSD), Springer International Publishing, https://link.springer.com/chapter/10.1057%2F9780230605572_7.

23. Shulsky, Abram N., Schmitt, Gary J., (2002), *Silent Warfare : Understanding the World of Intelligence*, 3rd ed., Washington, D.C.; London: Brassey's.

24. *The Romanian Intelligence Service Report on the Activity* (2012).

25. United Nations, (2000), *Report of the Secretary-General on the Implementation of the Report of the Panel on United Nations Peace Operations*, New York, October 20, para.96f (at www.un.org/peace/reports/peace_operations/ docs/55_502e.pdf).

INTERNATIONAL SECURITY ENVIRONMENT

CENTRAL ASIAN STATES: CATALYSTS FOR THE RUSSIAN-CHINESE NEW GREAT GAME

Claudia-Iohana VOICU

Mihail PĂDURARU

Abstract

The aim of this paper is to articulate the key role that small states play in the contemporary security architecture and how their strategies adapt to the dynamics of the geopolitical landscape. Using this analysis on Central Asia's New Great Game players as a frame of reference, we can further assess how leveraging its position between two spheres of influence can impact the development of a small nation's security.

As such, in the elaboration of this paper we studied the defence measures adopted by Central Asian states, with an emphasis on Turkmenistan, Uzbekistan and Tajikistan, with the support of either the Russian Federation or P.R. China and focused on their implications on a regional power game scale.

Keywords*: uncertainty, leverage, hedging, power games, New Great Game*

Motto: *"if Lilliputians can tie up Gulliver,*
or make him do their fighting for them,
they must be studied as carefully as the giant."
Keohane (1969, p. 310)

Introduction

Historical evolutions show us that small states are often limited in their ability to determine their own faith. Moreover, these patterns seem universal across all continents and periods of time. From this standpoint, Central Asian states could be compared to pawns on the grand chessboard of the regional political power players.[1]

After the fall of the USSR, the five newly formed sovereign states in Central Asia, Turkmenistan, Kazakhstan, Uzbekistan, Tajikistan and Kyrgyzstan, were engaged in a new silent competition to carve their identity and position in the regional security complex. While this complex is influenced to a certain

[1] Lena Jonson *Tajikistan in the New Central Asia. Geopolitics, Great Powers, Rivalry and Radical Islam*, (IB Tauris&CO Ltd, UK, 2006), p.3

extent by all the main players of the New Great Game, including states like Turkey, USA, Pakistan or Iran, its dynamics are mainly determined by two great powers which have a direct strategic interest in the region, each for their own reasons – the Russian Federation and the People's Republic of China.

In the international relations' theoretical models, the actions taken by a state to ensure its own security and protect its interests, often create uncertainty for the security of the surrounding states. As such, from a strategic perspective, any advance (in the defence sector) made by China outside of its pre-existent ties (mainly in the economic sector) to secure its interests in Central Asia could challenge Russia's status quo in the region. Naturally, the Russians respond symmetrically, escalating the issue and thus creating a chain of actions and reactions, which fall under the umbrella of the current security dilemma.

Furthermore, the small countries of Central Asia experienced first-hand the difficulties of building their nations whilst being on the frontline of an undeclared turf war between the Russians and the Chinese. However, as a survival mechanism, they learned to use this apparent vulnerability to advance their own agendas and adopted an active role in the security dilemma. In this paper, we will focus on three of these states: Turkmenistan, Tajikistan, Uzbekistan and follow how, by choosing to cooperate more heavily with one of the two main players to fulfil separate strategic objectives, they can alter the current power balance.

The purpose of the following study is to show how a small state can leverage its position between the Russian and Chinese spheres of influence by using a mixed strategy known as hedging and therefore ensures the external support needed from both players simultaneously. Moreover, while most scholars focus on the interests and strategies of the great players in the region, we will focus on the options of the smaller states and on their most advantageous strategies.

The paper starts by providing context on the latest evolutions in the geopolitical alliances formed in Central Asia and carries on to provide insight into the current strategies adopted by Turkmenistan, Uzbekistan and Tajikistan as the region slowly morphs into a complex multipolar system.

A new strategic approach

Context

As main actors of the regional security dilemma, the Russian and Chinese interests in the region shape the geopolitical scenery. While Russia continues to dominate the Central Asia defence sector and China the economic sector, the current policies are not linear and the traditional spheres of influence now often overlap, pressuring the smaller states to rethink their

former allegiances. For instance, Russia formed and leads the Collective Security Treaty Organization and takes part, together with China, in the Shanghai Cooperation Organization. However, to protect the security of its investments, China initiated the Quadrilateral Cooperation and Coordination Mechanism[2], a security mechanism that does not include Russia. Moreover, Russia also increased its influence in the economic sphere by expanding the cooperation in the CIS space- it created the Eurasian Economic Union, based on the EU model, which is a competitor of the Chinese Silk Road Economic Belt. Nevertheless, both countries refrain from directly antagonizing each other and are currently debating a common framework for the two economic initiatives.[3] In addition, we mention that due to its natural configuration, in this region the economic sector (energy, especially) and state security are often linked.

According to a vulnerability report published annually by the US based think tank the Fund for Peace, along with Foreign Policy, the Fragile States Index, all five Central Asian states have registered progress in their development over the past five years[4]. Furthermore, statistically, the security apparatus of all five countries followed a continuous upward trend for the last ten years, which shows an increase in overall state stability and security.[5] We will further assess the positioning within the Russian-Chinese security dilemma of three of the five Central Asian states.

The regional security complex formed in Central Asia during the past 25 years implies that each state must mould its defence policies by factoring in the interests and priorities of its neighbours. When discussing security issues in Central Asia, the focus will be on the states that border Afghanistan, the main source of instability for the region. As such, Turkmenistan, Uzbekistan and Tajikistan are linked to each other regardless of their historical and political differences due to several reasons – Firstly, their position as frontline states, with large minority groups living in Afghanistan and the return of the Central Asian fighters from the Islamic State[6] raises the risk of the potential

---

[2] *Afghanistan, China, Pakistan, Tajikistan issue joint statement on anti-terrorism*, Ministry of National Defense of the People's Republic of China, accessed 10 September 2017 at http://eng.mod.gov.cn/DefenseNews/2016-08/04/content_4707451.htm

[3] "Russia, China agree to integrate Eurasian Union, Silk Road, sign deals", *RT*, accessed 10 September 2017, https://www.rt.com/business/256877-russia-china-deals-cooperation/

[4] *Five-year trends*, Fragile States Index, accessed 10 September 2017, http://fundforpeace.org/fsi/decade-trends/five-year-trends/

[5] *Comparative Analysis,* Fragile States Index, accessed 10 September 2017, http://fundforpeace.org/fsi/comparative-analysis/

[6] Iris Oppelaar, "Central Asia and Islamic State: The Russian Connection", *The Diplomat,* accessed 6 August 2017, http://thediplomat.com/2017/03/central-asia-and-islamic-state-the-russian-connection/

spread of radical Islamism and internal destabilization. Secondly, from an economic standpoint, water scarcity makes the Amu Darya River[7] critical for Turkmenistan and Uzbekistan's agriculture sector and its use essential for ensuring Tajikistan's energy necessities in the upstream, thus making dialogue inevitable on the longer term, to ensure national and regional security and avoid the creation of a potential military conflict for vital resources. Thirdly, both from an economic and a military perspective, all three states form an important section that links the East to the West in the new infrastructure projects promoted by China, and in the initiatives promoted by Russia. As these projects develop, these three states start to cooperate to a certain extent[8] in order to capitalize their potential gains on one hand, while leveraging their potential benefits from both Russia and China, on the other.

Turkmenistan ranked 86th/178 countries analysed in the Fragile States Index, and it's not a member of neither the SCO nor the CSTO, and it did not sign the Paris Charter for OSCE, deepening its mandate. Moreover, the country has maintained a firm neutrality status recognized by the United Nations. Despite its positive neutrality doctrine, Ashgabat is now looking to modernize its military capabilities[9] and to diversify its suppliers. According to SIPRI[10], 36% of its weapons come from Turkey, 27% from China and 20% from Russia.

Authorities have reasons to be warry of a potential attack at their southern border, as there have been reports[11] of militant crossings into Turkmenistan as well as increased Taliban activity into the northern Afghan provinces. After a militant border attack that left several Turkmen soldiers dead, the country actively sought Russian military aid[12]. Moreover, in June

---

[7] Ramon E Collado, "Water War in Central Asia: the Water Dilemma of Turkmenistan", *Geopolitical Monitor*, accessed 11 September 2017, https://www.geopoliticalmonitor.com/water-war-in-central-asia-the-water-dilemma-of-turkmenistan/

[8] Bruce Pannier, "Is This The Start Of Regional Cooperation In Central Asia?", *RFEL,* accessed 11 September 2017, https://www.rferl.org/a/qishloq-ovozi-uzbekistan-mirziyaev-neighbors-cooperation/28506666.html

[9] "Isolationist Turkmenistan Is Rearming Too", *The 21st Century Arms' Race*, accessed 12 September 2017, https://21stcenturyasianarmsrace.com/2016/03/27/isolationist-turkmenistan-is-rearming-too/

[10] Joshua Kucera, "Report: Turkmenistan is Turkey's Biggest Weapons Buyer", *Eurasianet*, accessed 12 September 2017,
http://www.eurasianet.org/node/82476

[11] Bruce Pannier, "Is There A Terror Threat In Turkmenistan?", *RFEL*, accessed 12 September 2017, https://www.rferl.org/a/qishloq-ovozi-turkmenistan-terror-threat-afghanistan-islamic-state/28653368.html

[12] "Turkmenistan Seeks Military Aid From Russia", *Eurasianet*, accessed 12 September 2017, http://m.eurasianet.org/node/79151

2016, the Russian Defence Minister Sergei Shoigu visited Ashgabat to discuss[13] further security cooperation, weapons sales and tackling regional instability. In spite of the weakening of Russian-Turkmen relations following a spat with Gazprom on gas prices, Turkmenistan is still dependent on Russian support for its defence. In addition, Turkmenistan took part of NATO training programs to improve border security and was involved in the Northern Distribution Network used by the International Security Assistance Force in Afghanistan.

Neighbouring Uzbekistan ranked 63rd/178 in the Fragile States Index and 1st in terms of military strength among Central Asian States in the Global Fire Power rating for 2017[14]. It forms part of SCO, hosts its permanent counter-terrorism arm, the Regional Anti-Terrorism Structure, and, also, it expressed interest in strengthening economic ties with China within the BRI, which would bring much-needed large-scale funding for infrastructure development[15]. The country is particularly relevant for China, as it hosts a large Uyghur community, whose ties to the separatist movements in Xinjiang[16] have been a focal point for the Chinese policy in the region. What's more, Uzbekistan is no longer a member of the CSTO and it is not a member of the Eurasian Economic Union.[17] Nonetheless, the new regime of Mirziyoyev points to a restart in Russian-Uzbek relations, as the countries held this year the first joint bilateral military exercises in 10 years.[18] In addition, Uzbekistan expressed interest in supporting Russian peacekeeping missions in Afghanistan.[19]

---

[13] Paul Stronski, "Turkmenistan at Twenty-Five: The High Price of Authoritarianism", *Carnegie Endowment*, accessed 13 September 2017, http://carnegieendowment.org/2017/01/30/turkmenistan-at-twenty-five-high-price-of-authoritarianism-pub-67839

[14] Kamila Aliyeva, "Uzbek army strongest in the region - GFP rating", *TREND News Agency,* accessed 6 September 2017, https://en.trend.az/casia/uzbekistan/2792428.html

[15] Connor Dilleen, "China's Belt and Road Initiative in Central Asia: insurmountable obstacles and unmanageable risks?", *ASPI*, https://www.aspistrategist.org.au/chinas-belt-road-initiative-central-asia-insurmountable-obstacles-unmanageable-risks/

[16] *Why is there tension between China and the Uighurs?,* BBC World News, accessed 4 August 2017, http://www.bbc.com/news/world-asia-china-26414014

[17] Roncevert Ganan Almond, "Summits, Roads and Suspended Disbelief in Central Asia", *The Diplomat,* accessed 5 August 2017, http://thediplomat.com/2017/06/summits-roads-and-suspended-disbelief-in-central-asia/

[18] Joshua Kucera, "Uzbekistan and Russia to Restart Joint Military Exercises", *Eurasianet,* accessed 8 July 2017, http://www.eurasianet.org/node/84206

[19] Samuel Ramani, "Russia and Uzbekistan's Renewed Security Partnership", *The Diplomat,* accessed 11 September 2017, http://thediplomat.com/2017/07/russia-and-uzbekistans-renewed-security-partnership/

Uzbekistan has been one of the opaquest states in the region during the past 25 years and cooperation was restricted by the border demarcation disputes it had with Turkmenistan, Tajikistan and Kyrgyzstan, which have gone largely unsolved under the Karimov regime. However, the official new policy is to achieve greater regional cooperation and stability[20]. Uzbek authorities have already started settling part of the disputes, such as Kyrgyz-Uzbek border delimitation,[21] yet there are several other unsolved matters inherited from the old regime, such as the water disputes with Kyrgyzstan and Tajikistan, the Ferghana Valley's instability, securing the Afghan border and so on.

On its end, Tajikistan is the regional state with highest position in the Fragile States Index, 61st/178, and ranked last in terms of military power in the Global Fire Power rating of 2017. Also, economically, it depends on Russian and Chinese investments.

Reliant on Russia for its defence capabilities, Tajikistan is part of the CSTO and the SCO. Moreover, in 2016, Tajikistan joined China's first military initiative in Central Asia- the Quadrilateral Cooperation and Coordination Mechanism, that bypasses Russia, which is relevant as Tajikistan hosts the largest of Russia's military bases abroad[22], as well as an US military base[23]. The US holds annual exercises jointly with the host, Pakistan, Kyrgyzstan and Mongolia[24] and cooperates under the NATO Partnership for Peace framework. Additionally, in 2016, China held its first bilateral military exercise with Tajikistan, and funded the construction of a border guard training centre, 11 posts on the frontier and a joint Chinese-Tajik anti-terror centre in Dunshabe[25]. However, the Tajiks remain cautious as a latent territorial dispute

---

[20] *Briefing No 84 Uzbekistan: Reform or Repeat?,* The International Crisis Group, accessed 4 August 2017, https://www.crisisgroup.org/europe-central-asia/central-asia/uzbekistan/84-uzbekistan-reform-or-repeat

[21] "Uzbekistan and Kyrgyzstan preferred to resolve border issue secretly", *Eurasia News,* accessed 11 September 2017, http://eurasianews.info/en/important/uzbekistan-and-kyrgyzstan-preferred-to-resolve-border-issue-secretly.html

[22] "Stans undelivered", *The Economist*, accessed 5 August 2017, https://www.economist.com/news/asia/21701522-five-former-soviet-republics-struggle-survive-new-great-game-stans-undelivered

[23] Catherine Putz, "What Does CENTCOM Care About in Central Asia?", *The Diplomat,* accessed 7 August 2017, http://thediplomat.com/2017/03/in-2017-what-does-centcom-care-about-in-central-asia/

[24] Nadin Bahrom, "Joint military exercise underscores common challenges to Central Asia", *Central Asia News,* accessed 10 September 2017, http://central.asia-news.com/en_GB/articles/cnmi_ca/features/2017/07/21/feature-01

[25] Alexandr Kniazev, "*КАРТ-БЛАНШ. Китай приступает к созданию военного альянса в Центральной Азии*", *Nezavisimaya Gazeta*, accessed 10 August 2017, http://www.ng.ru/world/2016-03-15/3_kartblansh.html

led to allowing China annex over 1% of its territory[26] , which included the strategic Wakhan Corridor, and talks on the matter resurface periodically. Separately, Russia and its allies held in Tajikistan exercises that are usually conducted under the CSTO framework, this time under the Commonwealth of Independent States Anti-Terrorism Centre, which also includes former CSTO-member, Uzbekistan, indicating an improvement in Russian-Uzbek relations.[27]

Strategic Hedging – Central Asia's response to growing multi-polarity

As the reminiscent structures of the former USSR are slowly morphing so that Central Asian states adapt to an increasingly multipolar region, we also note a change in their defence strategies. The traditional main alignment options when faced with a security dilemma used to limit the smaller states' approaches to mostly traditional bandwagoning or balancing. However, the anarchic trend present in the regional security complex[28] and the historical mistrust these countries have between each other, meant that smaller states would need to adopt a pro-active role to fulfil their national strategic objectives.

A characteristic of the security dynamics of the region is the interlink between the economy and defence sectors. Consequently, both China and Russia, as the main players of the New Great Game use, on one hand, economic initiatives, such as the Silk Road Belt or the Economic Eurasian Union, and on the other, military alliances as vehicles to expand their spheres of influence regionally. This knowledge posed a challenge to the weaker Central Asian countries, whose agendas include both strengthening their own security and stability, as well as economic development and market access. However, neither continuing isolation, nor overt alignment with solely one player are feasible alternatives to achieve all their individual goals.

Therefore, as a reaction to the new geopolitical configuration, in order to amass all their opportunities without challenging Russia as the historical main player in the region, nor antagonize China, the largest regional investor, smaller states like Turkmenistan, Uzbekistan and Tajikistan have adopted a mix of strategies known as hedging, which combine elements of the more traditional approaches, such as bandwagoning or high-intensity balancing.

---

[26] Fuad Shahbazov, "China's Economic and Military Expansion in Tajikistan", *The Diplomat,* accessed 3 August 2017, http://thediplomat.com/2016/11/chinas-economic-and-military-expansion-in-tajikistan/

[27] Joshua Kucera, "Russia Holds Military Exercises in Tajikistan -- But Why Not With CSTO?", *Eurasianet,* accessed 11 September 2017, http://www.eurasianet.org/node/83781

[28] Robert Jervis, "Cooperation under the Security Dilemma", *World Politics,* Vol. 30, Issue 2, 1978, pp 167-214

In the classical sense described by the international relations theories[29], bandwagoning would entail a clear strategic alignment with one state and its interests, either Russia or China, whilst balancing would imply an alignment with other regional states in response to the rise of a new larger player, here meaning China. Neither is suitable by itself for the priorities of smaller Central Asian countries in the current regional landscape. Firstly, both theories limit these states' capacity to adopt a more active role in engaging all the players that partake in the New Great Game. This is one of the reasons which led Uzbekistan to exit the CSTO in 2012. Secondly, bandwagoning would restrict which economic and military alliance a smaller state can approach. Moreover, as we have shown, neither of the three (Turkmenistan, Uzbekistan, Tajikistan) have shown complete alignment with either Russia, nor with China. Trends indicate that each state prefers to cooperate bilaterally on defined issues and avoid falling under the umbrella of a sole player. Thirdly, while all three states do apply certain elements of internal and external balancing in increasing both their military power, as well as form certain alliances, particularly to tackle the Taliban and Jihadi threat, mistrust and suspicion of the intentions of their neighbours mean that all observed states generally avoid fully integrating in rule-based regional organizations. Bilateral engagements are preferred instead. However, some exceptions do apply for example in Tajikistan, as the country's weak military cannot properly secure its borders and requires a high degree of assistance. Nevertheless, it is not advantageous for either of the three countries analysed to overtly balance against China, the challenger of the regional hierarchy, as they all depend economically on its investments, especially in the context of Russia's current economic decline. Nor is it advantageous to do so against Russia, as they depend on its military assistance, market, and on the remittances from Central Asian migrants' seasonal work on Russian soil.

Hedging initially appeared as an evolved soft balancing method, which allows a weaker state to improve its competitiveness while avoiding confrontation with larger players[30]. This strategy comprises a mix of measures that allow policy shifts from one issue to another, according to the state's best interest. Some analysts argue that hedging is most advantageous for smaller, weaker states that are more likely to prefer limited cooperation over zero-sum games in security matters.[31]

---

[29] Stephen Walt, "Alliances: Balancing and Bandwagoning", accessed 15 July 2017, available at http://www.ou.edu/uschina/texts/WaltAlliances.pdf

[30] Gustaaf Geeraerts, Mohammad Salman, "Measuring Strategic Hedging Capability of Second-Tier States Under Unipolarity", *Chinese Political Science Review*, Vol.1, No.1, 2016, pp. 62

[31] Evelyn Goh, "Understanding "hedging" in Asia-Pacific security", *PacNet*, No 43, 2006, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/pac0643.pdf

Central Asia's circumstances are similar to those of Southeast Asian[32] states, which are caught mainly between the Chinese and American spheres of influence. As such, the common patterns[33] between the two regions are not aligning overtly in favour of one major player, even though each state's objectives and general strategies may vary. ASEAN states such as Malaysia[34] have long adopted a hedging strategy as response to China's regional engagement, and chose to cooperate with both major powers to strengthen their security and stability. However, the Asian hedging trends differ from the mainly balancing strategies adopted by smaller states in regions such as the Middle East, which become clear in their policies towards Iran, for example.

By adopting an early strategic hedging measurement overview[35], we note that Central Asian states' policies are an answer to the changes in the regional power balance and the uncertainty that comes with it. First of all, all three countries maintain cooperation with Russia, the current dominant leader, on specific issues, while at the same time they adopt supply and demand diversification policies in order to decrease dependency in vital sectors, such as energy exports or arms purchasing. Second of all, all three countries are taking measures to improve their military capabilities and bilateral alliances in order to build resilience in case of the potential loss of Russian security assistance, thus, actively altering the current regional military balance. Nevertheless, Russia still dominates the defence sector, particularly as the disintegration of the Islamic State rose concerns regarding the implications of the Central Asian's Jihadi's return to their native countries. Moreover, Sinophobia is still present in the region, making smaller states suspicious of China's intense economic and military endeavours. The questions are multiplied by restrictive Chinese policies, such as imposing Chinese national workers in building the infrastructure projects financed through the BRI.

After gaining its independence, Turkmenistan had an atypical evolution. To protect its territorial integrity, it chose to adopt a positive

---

32 Ollii Suorsa, "Maintaining a Small State's Strategic Space: Omnidirectional Hedging" *International Studies Association Hong Kong*, accessed 14 July 2017, http://web.isanet.org/Web/Conferences/HKU2017-s/Archive/f40db849-cb90-4826-9b7a-e449b602f398.pdf

33 Evelyn Goh, "Southeast Asian Strategies toward the Great Powers: Still Hedging after All These Years?", *The ASAN Forum,* accessed 10 July 2017, http://www.theasanforum.org/southeast-asian-strategies-toward-the-great-powers-still-hedging-after-all-these-years/

34 CHENG-CHWEE, K. (2008)."The Essence of Hedging: Malaysia and Singapore's Response to a Rising China.", *Contemporary Southeast Asia, 30*(2), pp 159-185

35 Gustaaf Geeraerts, Mohammad Salman, "Measuring Strategic Hedging Capability of Second-Tier States Under Unipolarity", *Chinese Political Science Review*, Vol.1, No.1, 2016, pp. 62

neutrality doctrine and to position itself as a peaceful and stable pylon in a region fuelled by territorial and interethnic disputes. This policy allowed the country to avoid regional military alliances and, as such, it did not need to neatly adopt a traditional bandwagoning or balancing approach to ensure its defence needs. However, Turkmenistan has been dependent on Russian aid to secure its territory, arms purchasing and troops training. In addition, due to the Turkmen's proactivity to border security and Taliban threats, we can eliminate buck-passing as main strategy as well. Its security is built on bilateral alliances, yet it does not currently limit itself to cooperating with a single major power. It cooperates with Russia to compensate their defence capabilities' shortages, with China and Turkey for weapon's purchase, with Pakistan for ensuring the security of its strategic TAPI project construction. Therefore, Turkmenistan hedges based on its official neutrality to secure military assistance from various players without making any formal commitment. Noteworthy, security is intrinsically linked to the vital energy sector, which will affect the country's behaviour and regional ties, proof of which is a spike in weapons purchase diversification, which were formerly obtained from Russia, after the Russians stopped Turkmen gas imports. Despite this, as the small Caspian state does not have the full military capabilities necessary to respond to the increase in Taliban activity at its southern border, it has continued a close military cooperation with the Russian Federation. Additionally, it responded to the disadvantageous demands of the Russian's regarding gas prices by increasing cooperation with China instead.

Uzbekistan, on the other hand, under Karimov's regime isolated itself both from its neighbours, as well as from former major allies and, as a consequence, it did not actively seek a pivotal role, as it could have, in the Russian-Chinese security dilemma. However, under its new leadership, Uzbekistan has made significant changes in its foreign policy and security priorities, its reach to both Russia and China indicating a similar choice to that of Turkmenistan and Tajikistan of leveraging its position to gain a more competitive advantage in the region. Its geographical position, resources and powerful military makes it essential to both military and economic alliances forged by China and Russia.

Though the early defence strategy of Tajikistan was bandwagoning, its strategic position at the frontline of the Afghan conflict, internal turbulence, the multipolar New Great Game evolutions and the periphery position in Russia's backyard meant that the country could leverage its weak, non-threatening position to gain significant more military and economic aid from all the countries that had an interest in easy access to Afghanistan. Therefore,

the Tajik government increased military cooperation both with Russia and with China, as well as with the United States. However, as bandwagoning was no longer advantageous and sole balancing not feasible on the long term, a mix of strategies was preferred. As such, Tajikistan remains one of Russia's closest allies in Central Asia, yet it simultaneously entered a newly formed military alliance with China that excludes it and the NATO Partnership for Peace. Thus, contrasting its neighbours, the Tajiks adopt omnidirectional hedging as they try to maximize military aid and capitalize any investments that are made on their territory.

Conclusions

To sum up and conclude, the mixed strategy adopted by Central Asian countries is a result of the increased uncertainty, mistrust, and caution towards the regional ambitions of New Great Game players, as well as an intention to leverage their position to gain a more advantageous role in the changing configuration. Since the complexity and high interdependence of the regional relations prevent overt alignment with either Russia or China, all three states analysed are expected to hedge between both players, using specific needs that change from issue to issue as incentive.[36]

As a consequence, small states such as Turkmenistan, Uzbekistan and Tajikistan will play a more active role in security dilemmas caused by similar dynamics, as their alignment options on either defence or economic matters could cause a shift in the regional power balance and intentionally allow a significant overlap of spheres of influence.

Moreover, as frontline states to an active warzone, all three countries will and should have as priority to advance their security agenda, while their choices could destabilize the entire region. The security risks are heightened by the persistent Taliban threat, interethnic tensions, and the risk of Islamic radicalization. The latter is caused by the return of Central Asian fighters back home after Daesh's loss of terrain and financing, and fostered by both the precarious economic conditions that increase popular restlessness, as well as the severe crackdown on Islamic symbols and traditions in countries such as Tajikistan. In addition, Russia's justifications for the recent territorial annexations in Ukraine and military doctrine have caused concerns of a potential scenario being repeated in Central Asia, as the significant size of the Russian communities there could create an incentive for Moscow for an

[36] Van Jackson, "The Rise and Persistence of Strategic Hedging across Asia: A System-Level Analysis", *Strategic Asia 2014-2015, US alliances and partnerships at the Center of Global Power, The National Bureau of Asian Research, 2014*

intervention if the instability level increases. Also, Uzbekistan's large Uyghur community has caused friction in its relationship with China, as the latter has been accused of interfering into the small country's internal affairs by demanding a tighter supervision of this minority's activity and ties to the Uyghur in Xinjiang.

Strategic hedging between the main players to maximize opportunities is the key for these small Central Asian states to strengthen their defence and maintain a stable environment. This would allow the current regimes to further develop their countries and prevent any foreign intervention or military conflict on their territory. However, their decisions and alliances should be chosen wisely and in accordance with the strategic agenda of big actors such as Russia and China.

Turkmenistan, Uzbekistan and Tajikistan chose to hedge between large players to protect their national integrity, but how will Russia or China react when a decision of one of these states would affect its regional interests?

References:

1. *Afghanistan, China, Pakistan, Tajikistan issue joint statement on anti-terrorism*, Ministry of National Defense of the People's Republic of China, accessed 10 September 2017 at http://eng.mod.gov.cn/DefenseNews/2016-08/04/content_4707451.htm

2. Aliyeva, Kamila, "Uzbek army strongest in the region - GFP rating", *TREND News Agency,* accessed 6 September 2017, https://en.trend.az/casia/uzbekistan/2792428.html

3. Bahrom, Nadin, "Joint military exercise underscores common challenges to Central Asia", *Central Asia News,* accessed 10 September 2017, http://central.asia-news.com/en_GB/articles/cnmi_ca/features/2017/07/21/feature-01

4. *Briefing No 84 Uzbekistan: Reform or Repeat?,* The International Crisis Group, accessed 4 August 2017, https://www.crisisgroup.org/europe-central-asia/central-asia/uzbekistan/84-uzbekistan-reform-or-repeat

5. Cheng-Chwee, K. (2008)."The Essence of Hedging: Malaysia and Singapore's Response to a Rising China.", *Contemporary Southeast Asia, 30*(2), pp 159-185

6. Collado, Ramon E., "Water War in Central Asia: the Water Dilemma of Turkmenistan", *Geopolitical Monitor*, accessed 11 September 2017, https://www.geopoliticalmonitor.com/water-war-in-central-asia-the-water-dilemma-of-turkmenistan/

7. *Comparative Analysis,* Fragile States Index, accessed 10 September 2017, http://fundforpeace.org/fsi/comparative-analysis/

8. Dilleen, Connor, "China's Belt and Road Initiative in Central Asia: insurmountable obstacles and unmanageable risks?", *ASPI*, https://www.aspistrategist.org.au/chinas-belt-road-initiative-central-asia-insurmountable-obstacles-unmanageable-risks/

9. *Five-year trends*, Fragile States Index, accessed 10 September 2017, http://fundforpeace.org/fsi/decade-trends/five-year-trends/

10. Geeraerts, Gustaaf, Mohammad Salman, "Measuring Strategic Hedging Capability of Second-Tier

11. States under Unipolarity", *Chinese Political Science Review*, Vol.1, No.1, 2016, pp. 62

12. Goh, Evelyn, "Southeast Asian Strategies toward the Great Powers: Still Hedging after All These Years?", *The ASAN Forum,* accessed 10 July 2017, http://www.theasanforum.org/southeast-asian-strategies-toward-the-great-powers-still-hedging-after-all-these-years/

13. Goh, Evelyn, "Understanding "hedging" in Asia-Pacific security", *PacNet*, No 43, 2006, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/pac0643.pdf

14. "Isolationist Turkmenistan Is Rearming Too", *The 21st Century Arms' Race*, accessed 12 September 2017, https://21stcenturyasianarmsrace.com/2016/03/27/isolationist-turkmenistan-is-rearming-too/

15. Jervis, Robert, "Cooperation under the Security Dilemma", *World Politics,* Vol. 30, Issue 2, 1978, pp 167-214

16. Jonson, Lena, *Tajikistan in the New Central Asia. Geopolitics, Great Powers, Rivalry and Radical Islam*, (IB Tauris&CO Ltd, UK, 2006), p.3

17. Kniazev, Alexandr, "*КАРТ-БЛАНШ. Китай приступает к созданию военного альянса в Центральной Азии*", *Nezavisimaya Gazeta*, accessed 10 August 2017, http://www.ng.ru/world/2016-03-15/3_kartblansh.html

18. Kucera, Joshua ,"Report: Turkmenistan is Turkey's Biggest Weapons Buyer", *Eurasianet*, accessed 12 September 2017, http://www.eurasianet.org/node/82476

19. Kucera, Joshua, "Uzbekistan and Russia to Restart Joint Military Exercises", *Eurasianet,* accessed 8 July 2017, http://www.eurasianet.org/node/84206

20. Kucera, Joshua, "Russia Holds Military Exercises in Tajikistan -- But Why Not With CSTO?", *Eurasianet,* accessed 11 September 2017, http://www.eurasianet.org/node/83781

21. Oppelaar, Iris, "Central Asia and Islamic State: The Russian Connection", *The Diplomat,* accessed 6 August 2017, http://thediplomat.com/2017/03/central-asia-and-islamic-state-the-russian-connection/

22. Pannier, Bruce, "Is This The Start Of Regional Cooperation In Central Asia?", *RFEL,* accessed 11 September 2017, https://www.rferl.org/a/qishloq-ovozi-uzbekistan-mirziyaev-neighbors-cooperation/28506666.html

23. Pannier, Bruce, "Is There A Terror Threat In Turkmenistan?", *RFEL*, accessed 12 September 2017, https://www.rferl.org/a/qishloq-ovozi-turkmenistan-terror-threat-afghanistan-islamic-state/28653368.html

24. Putz, Catherine, "What Does CENTCOM Care About in Central Asia?", *The Diplomat,* accessed 7 August 2017, http://thediplomat.com/2017/03/in-2017-what-does-centcom-care-about-in-central-asia/

25. Ramani, Samuel, "Russia and Uzbekistan's Renewed Security Partnership", *The Diplomat,* accessed 11 September 2017, http://thediplomat.com/2017/07/russia-and-uzbekistans-renewed-security-partnership/

26. Roncevert, Ganan Almond, "Summits, Roads and Suspended Disbelief in Central Asia", *The Diplomat,* accessed 5 August 2017, http://thediplomat.com/2017/06/summits-roads-and-suspended-disbelief-in-central-asia/

27. "Russia, China agree to integrate Eurasian Union, Silk Road, sign deals", *RT*, accessed 10 September 2017, https://www.rt.com/business/256877-russia-china-deals-cooperation/

28. Shahbazov, Fuad, "China's Economic and Military Expansion in Tajikistan", *The Diplomat,* accessed 3 August 2017, http://thediplomat.com/2016/11/chinas-economic-and-military-expansion-in-tajikistan/

29. "Stans undelivered", *The Economist,* accessed 5 August 2017, https://www.economist.com/news/asia/21701522-five-former-soviet-republics-struggle-survive-new-great-game-stans-undelivered

30. Stronski, Paul, "Turkmenistan at Twenty-Five: The High Price of Authoritarianism", *Carnegie Endowment*, accessed 13 September 2017, http://carnegieendowment.org/2017/01/30/turkmenistan-at-twenty-five-high-price-of-authoritarianism-pub-67839

31. Suorsa, Ollii, "Maintaining a Small State's Strategic Space: Omnidirectional Hedging" *International Studies Association Hong Kong*, accessed 14 July 2017, http://web.isanet.org/Web/Conferences/HKU2017-s/Archive/f40db849-cb90-4826-9b7a-e449b602f398.pdf

32. "Turkmenistan Seeks Military Aid From Russia", *Eurasianet*, accessed 12 September 2017, http://m.eurasianet.org/node/79151

33. „Uzbekistan and Kyrgyzstan preferred to resolve border issue secretly", *Eurasia News,* accessed 11 September 2017, http://eurasianews.info/en/important/uzbekistan-and-kyrgyzstan-preferred-to-resolve-border-issue-secretly.html

34. Van Jackson, "The Rise and Persistence of Strategic Hedging across Asia: A System-Level Analysis", *Strategic Asia 2014-2015, US alliances and partnerships at the Center of Global Power, The National Bureau of Asian Research, 2014*

35. Walt, Stephen, "Alliances: Balancing and Bandwagoning", accessed 15 July 2017, available at http://www.ou.edu/uschina/texts/WaltAlliances.pdf

36. *Why is there tension between China and the Uighurs?,* BBC World News, accessed 4 August 2017, http://www.bbc.com/news/world-asia-china-26414014

SECURITY STRATEGIES AND POLICIES

THE POLISH INTELLIGENCE SERVICES AND SECURITY DILEMMAS OF A FRONTLINE STATE

Artur GRUSZCZAK *

Abstract

This paper seeks to analyze the dynamics of Poland's intelligence sector reform following the 2015 general elections and present tasks and challenges facing the Polish intelligence services. In the aftermath of presidential and parliamentary elections in 2015, the long period of liberal dominance was ended with the triumph of nationalist conservative Law and Justice Party. Illiberal elements incorporated into democratic governance have raised numerous concerns and official warnings from the European Commission. In parallel, strong support for NATO reinforcement, growing military spending and important changes in the national defence system (establishment of territorial defence forces) have appeased the critical voices and rescued Poland from isolation in the transatlantic security system. The new government has constantly highlighted Poland's position as a frontline state vis a vis Russia and its close ally – Belarus. Moreover, neighbourhood with war-torn Ukraine has added more risks to geostrategic location. In this complex environment, Poland's intelligence services have also undergone important changes: personnel reshuffling, politicization and partial reorganization. The paper aims at examining the capacity of Poland as a middle European state to cope effectively with security problems and challenges emerging from both internal political dynamics and external strategic shifts.

Keywords*: Poland, special services, Law and Justice Party, security, defence, intelligence reform*

Introduction

After the long 8-year period of liberal rule in Poland, the 2015 presidential and parliamentary elections brought about a true seachange in

* Associate Professor, Jagiellonian University, Kraków, Poland, artur.gruszczak@uj.edu.pl

Polish politics, including defence policy and intelligence sector.[1] The victory of conservative Law and Justice (Prawo i Sprawiedliwość – PiS) party, under Jarosław Kaczyński strong-hand leadership, meant the beginning of a deep transformation of the political regime toward illiberal democracy saturated with nationalist discourse and confrontational posture both on the domestic political stage and in the international arena.[2] Although PiS's electoral triumph and the high popular support maintained since the elections have been the effect of inertia of the former liberal Civic Platform in the last period of its rule and weaknesses as the main opposition party after 2015, the strong position of PiS in the party system and political life raises a query of its impact on Poland's security strategy, defence policy and international posture as the NATO and EU member state. Consequently, it entails the issue of organization, performance and effectiveness of intelligence services.

The 2015 political change and its consequences for Poland's security policy and strategy

Poland's foreign policy has undergone a significant and substantive reconfiguration after 2015. Heavily critical of its predecessors, the Szydlo government introduced under the slogan „getting up off our knees" a clear nationalist posture and a much more assertive, even hardened posture on external relations. First of all, Poland challenged the EU's policies and principles with regard to asylum and migration, environmental protection and rule of law. Moreover, having implemented some elements of illiberal democracy in the political system, it provoked growing concerns among EU institutions: the European Commission and the European Parliament. A confrontational stance adopted by the Polish government led to escalation of reactions of these institutions, including the possibility of triggering the sanction procedure under Article 7 TEU.[3] A more defiant position was demonstrated in form of disobedience to the decision of the Court of Justice of the EU on adopting interim measures concerning suspension by the Polish

---

[1] See: Krzysztof Jasiewicz, Agnieszka Jasiewicz-Betkiewicz, "Poland" *European Journal of Political Research Political Data Yearbook* Vol. 55, 2016, pp. 204–215; Radosław Markowski, "The Polish parliamentary election of 2015: a free and fair election that results in unfair political consequences" *West European Politics*, Vol. 39, No. 6, 2016, pp. 1311–1322.

[2] Jakub Dymek, "Poland's Rightward Turn" *Dissent*, Vol. 63, No. 2, 2016, pp. 123-127.

[3] Eszter Zalan, "EU Commission sets red lines for Poland on Article 7", *EU Observer.com*, 26 July 2017, accessed 28 July 2017 at https://euobserver.com/political/138618.

authorities of intensive logging in the Białowieża Forest, which is a protected Natura 2000 and Unesco World Heritage site.[4]

The above mentioned examples of anti-EU stance stem from deeper structural prerequisites, strongly embedded in the mind set of PiS's leadership. The concept of counterrevolution, vowed by Jarosław Kaczyński, the chairman of Law and Justice, entails a deep revision of norms, values and attitudes dominating in Western Europe and their replacement by traditional ideological, societal and economic patterns, specific for countries of Central Europe long located on the periphery of the "modern" Europe. Counterrevolution directly addresses Europeanisation as a process of cultural modernisation and socio-economic transformation. It opposes supranational mechanisms of EU governance, deregulatory mechanisms of the common market, harmonisation of laws and the current institutional setting of the EU. European integration, according to Kaczyński, brought about a "gigantic cultural degradation". The European Union in order to survive must be constituted on national and religious values which should be an integral part of "European documents."[5].

Although conservative, nationalist, sometimes xenophobic discourse has proliferated across the European Union, it was employed by smaller parties, not represented in the government, except Poland and other Central European countries: Hungary, Slovakia and the Czech Republic, forming the so-called Visegrad Four (V4). Given that the Orban government in Hungary has been an influential reference pattern for the Law and Justice party, the Polish-Hungarian alliance has been considered as the cornerstone of Poland's foreign policy. It was also a safeguard against the EU's growing irritation at Poland's defiant position in matters requiring unanimity in the Council of the EU. This has been particularly relevant in the face of deteriorating relations between Poland and the two "engines" of European integration: Germany and France.

Anti-German attitudes in Polish society were explored for the sake of electoral campaigns and popular mobilization around PiS's political projects. Germany was blamed for the migration crisis in Europe and – indirectly – the growing insecurity and terrorist threats. In historical context, it was portrayed as an unsolved nation which managed to avoid a

---

[4] Ordonnance du Vice-Président de la Cour, 27 juillet 2017, dans l'affaire C-441/17 R, accessed 28 July 2017 at http://curia.europa.eu/juris/document/document.jsf?text&docid=193373&pageIndex=0&doclang=FR&mode=req&dir&occ=first&part=1&cid=455841.

[5] Jacek Karnowski, "Europejska (kontr)rewolucja" *W Sieci*, 12-18 September 2016, p. 28.

just punishment for the horrible crimes and atrocities committed during World War II. As a result, PiS demanded war reparations estimated at close to $1 trillion.[6]

France has been criticized for anti-Polish motives in Emmanuel Macron's presidential campaign, concerning labour migration in the EU, especially posted workers from Poland, illiberal elements of PiS's rule and – last but not least – the questioning of "European values" by the Polish government. As the president of France, Macron marginalized Poland not only in the EU, but even in the central and eastern part of the Union. During his tour of Central and Eastern Europe in August 2017, he steered clear of Poland. While in Bulgaria, he commented that Poland is "a country that has decided to go against European interests in many areas" and added that it is "placing itself on the margins of Europe's future history".[7] France's criticism of the Polish authorities has addressed yet another controversial issue. The Szydlo government decided in October 2016 to cancel a $3.5-billion deal with Airbus Helicopters for 50 military multi-role Eurocopters EC725 "Caracal" which had been concluded by the former liberal government. Negotiations of a proposed offset agreement were broken off in suspicious circumstances by representatives of the controversial Defence Minister Antoni Macierewicz.[8] French president Hollande and his defence minister indefinitely postponed their visit to Warsaw scheduled for October 2016 and the relations between the two countries rapidly deteriorated.

Polish foreign policy traditionally has been pro-American. From the beginning of the 21st century, Poland has considered the United States as its strongest ally, the key actor in the Euro-Atlantic security system and guardian of its national security. Despite certain reservations regarding the Bush and

---

[6] "Poland could seek war reparations from Germany, say parliament researchers" *Politico*, 11 September 2017, accessed on 14 September 2017 at http://www.politico.eu/article/poland-could-seek-war-reparations-from-germany-say-parliament-researchers/; "The Polish government is seeking $1trn in war reparations from Germany" *New Statesman*, 18 September 2017, accessed 20 September 2017 at https://www.newstatesman.com/culture/observations/2017/09/polish-government-seeking-1trn-war-reparations-germany.

[7] "Emmanuel Macron called 'arrogant' and 'inexperienced' by Polish prime minister Beata Szydlo in worker spat" *The Telegraph*, 25 August 2017, accessed 28 August 2017 at http://www.telegraph.co.uk/news/2017/08/25/emmanuel-macron-called-arrogant-inexperienced-polish-prime-minister/.

[8] "Polish defence minister denies overstepping powers" *Radio Poland*, 9 May 2017, accessed 28 August 2017 at http://www.thenews.pl/1/9/Artykul/306113,Polish-defence-minister-denies-overstepping-powers.

Obama administrations, Poland consistently supported U.S. global strategy.[9] However, following the 2015 political change in Poland, U.S.–Polish diplomatic relations turned sour and reached a bottom during President Obama's visit to Warsaw on the occasion of NATO summit in July 2016. Barack Obama rebuked Polish leaders over changes in the Constitutional Court and a presumed violation of standards regarding the rule of law.[10] The electoral victory of Donald Trump was enthusiastically welcomed by the Polish right-wing sector. Despite his personal connections with Russia's top officials, he was praised for anti-immigrant stance, distance from EU integration and criticism of European allies paying too little for the collective defence under NATO's umbrella. Moreover, his passionate history-saturated speech in Warsaw during an official visit to Poland in July 2017 caused tremendous excitement among the Polish authorities and the national-conservative sector of society.[11]

Good relations with the United States have been considered as a priority also for Poland's security policy and strategy. Polish foreign policy strategy for the years 2017-2021, adopted in July 2017, put it straightforwardly: "Both within NATO and bilaterally, Poland will seek to reinforce its defence partnership with the United States, particularly with respect to US military presence in Poland and more broadly, across the entire eastern flank. American military involvement in Europe is key to maintaining NATO's collective defence and deterrence capabilities."[12] This is particularly important in the context of main threats to Poland's security which were located on NATO's Eastern flank: Russia's aggressive stance, armed conflict in eastern Ukraine, Belarus's submission to the Russian expansive interests. Therefore, Polish government strove for NATO's greater interest in strengthening the Eastern flank and bigger involvement in defence capacities. NATO's summit in Warsaw in July 2016 brought satisfactory results to the host country. The Alliance agreed on the military adaptation on the Eastern

---

[9] See Artur Gruszczak, "Poland: A Skillfull Player", in Eleanor E. Zeff, Ellen B. Pirro (eds), *The European Union and the member states* (Boulder, CO – London: Lynne Rienner Publishers, 2015, 3rd ed.), pp. 259-278.

[10] "Obama Rebukes Poland's Right-Wing Government" *The New York Times*, 8 July 2016, accessed 28 August 2017 at https://www.nytimes.com/2016/07/09/world/europe/obama-poland-nato-summit.html.

[11] "Right-Tilting Poland Welcomes Trump as Europe Watches Warily" *The New York Times*, 5 July 2017, accessed 28 August 2017 at https://www.nytimes.com/2017/07/05/world/europe/poland-trump-visit-g20.html.

[12] Ministry of Foreign Affairs, Republic of Poland, *Polish Foreign Policy Strategy 2017-2021*, pp. 6-7, accessed 14 September 2017 at http://www.msz.gov.pl/resource/0c98c3b2-9c5d-4c42-8761-f7827134ee76:JCR.

flank including the deployment of four multinational battalions with extended military tasks. One of them, to the satisfaction of the Polish government, will be stationed in Poland and – moreover – be composed of U.S. troops.

Although Poland – backed by the United States – attained its key security policy objective: a permanent NATO military presence on Polish territory, it has been marginalized in the European arena due to the disagreements with France and Germany over regional and European issues. As a form of compensation, in 2016 it launched along with Croatia the Three Seas Initiative[13] built upon the core V4 (Visegrad Four) Group. However, this community is substantially diversified and a traditional geopolitical view on the eastern part of Europe is its lowest common denominator.[14] Its security potential and military capabilities are fairly limited. The catalogue of threats and risks is quite heterogeneous and the attitude toward Russia rather mixed.

The above outlined portrayal of Poland's security features carries far-reaching implications for the Polish intelligence community. Firstly, the change of government in 2015 resulted in politicization of security sector and intelligence services, bringing about important personal and institutional alterations. Secondly, those changes weakened the potential and capabilities of intelligence and defence structures as well as complicated international collaboration links with major European allies. Thirdly, apart from the deficit of official information, one should acknowledge that foreign services, particularly Russian intelligence, have been increasingly active in Poland, particularly in the cyber/communication space, seeking to undermine Poland's position in NATO, weaken cooperation with EU institutions and enhance anti-Ukrainian attitudes. This constitutes a real challenge to Polish counterintelligence capacities and tests Poland's resistance to growing activities of adverse intelligence forces.

The organization and performance of the Polish intelligence services

Poland's intelligence community is relatively complex – in terms of a middle European power – and considerably diversified. Devoid of precise

---

[13] Apart from the Visegrad Four, the Three Seas Initiative was backed by the Baltic States (Estonia, Latvia and Lithuania), several Balkan countries (Slovenia, Croatia, Romania, Bulgaria) and Austria. See: Geostrategic Insights Into the Joint Polish-Croatian "Three Seas Initiative", accessed 14 September 2017 at https://www.globalresearch.ca/geostrategic-insights-into-the-joint-polish-croatian-three-seas-initiative/5598048.

[14] See Kamil Zwolski, "Poland's Foreign-Policy Turn" *Survival*, Vol. 59, No. 4, 2017, pp. 172-173.

normative bases and clear organizational framework, it encompasses numerous institutions and agencies which are at least partially involved in intelligence activities. Moreover, the scope of competencies and duties is not always well established which may lead to overlapping or – in extreme cases – conflicting activities. While territorial division of competencies is generally clear, with foreign intelligence agencies possessing exclusive powers to act abroad, homeland intelligence is an area dominated by a plethora of agencies, services and bodies. Part of them is focused on external threats, performing the functions of counterintelligence; others deal with criminal intelligence, engaging numerous law enforcement bodies; and yet others try to handle new intelligence challenges, such as cyber threats or progress in artificial intelligence.[15]

Intelligence is the principal domain of special services. In the Polish legal system[16] five institutions are recognized as "special services": (1) Internal Security Agency; (2) Foreign Intelligence Agency, (3) Military Intelligence Service, (4) Military Counterintelligence Service and (5) Central Anti-Corruption Bureau. They are authorized to collect, process and disseminate information and intelligence acquired or produced by covert means or methods. Moreover, the 2002 Law on the Internal Security Agency and the Foreign Intelligence Agency in Article 12 lists other entities involved in the protection of state security, among them the Police, Gendarmerie (Military Police), Border Guard, Customs Service, Government Protection Office, treasury chambers, tax authorities and intelligence and reconnaissance units of the Armed Forces. Some intelligence functions are granted to them in order to enable their co-operation with the special services with regard to intelligence and information security of the state in the preventive and investigative contexts. What is more, some specialized institutions and bodies undertake certain intelligence activities. One should mention the General Inspectorate of Financial Information - a unit of financial intelligence within the Ministry of Treasury; the Government Protection Office – a uniformed and armed service tasked with the protection of VIPs and respective facilities and

---

[15] See more: Artur Gruszczak, "Poland: The Special Services Since the Independence", in Bob de Graaff, James M. Nyce (eds.), *Handbook of European Intelligence Cultures* (Lanham: Rowman & Littlefield, 2016), pp. 279-290; Stéphane Lefebvre, "Poland's Attempts to Develop a Democratic and Effective Intelligence System, Phase 1: 1989–1999" *International Journal of Intelligence and CounterIntelligence*, Vol. 29, No. 3, 2016, pp. 470-502.

[16] The respective legal acts are: The 2002 Law on the Internal Security Agency and the Foreign Intelligence Agency, the 2006 Law on the Military Counterintelligence Service and the Military Intelligence Service and the 2006 Law on the Central Anti-Corruption Bureau.

infrastructure; the Special Operation Forces Command – the special forces command integrating five elite commando units involved in special operations home and abroad and developing the required intelligence support.

The above listed numerous agencies and entities have been tasked with differentiated goals, duties and missions scattered across various areas of state activities in the area of security and defence. Their main objective is **c**ollection, analysis, processing and delivery to relevant authorities of information which may be vital for the state's security, its constitutional order, economic and defence potential, elements of critical infrastructure as well as international position. The resulting intelligence products should enable an appropriate and effective identification and countering of major threats to national defence, security and combat capacity of the Armed Forces, international terrorism, extremism and organized crime, proliferation of weapons of mass destruction as well as threats emerging in the areas of international tensions, conflicts and crises.

The management of such a vast institutional structure has not been an easy task. Although formally subordinated to the head of government, the secret services and other intelligence-related bodies fall under specific competences of relevant ministers, subject to their prerogatives and the range of activities. The Prime Minister enacts statute to each of the secret services, appoints and recalls their heads after consultations with the President, the Board for Special Services and the Parliamentary Committee for Special Services. The Prime Minister also issues binding directives and requests information and opinion from the heads of the secret services as well as the Minister for Internal Affairs – with regard to civilian intelligence bodies and Minister of National Defence – with reference to the military branch of intelligence and counterintelligence.

The defence intelligence organizations have kept a specific profile in the system of special services due to their institutional affiliation, international obligations and sensitivity of matters and areas of their concern. They have striven to distinguish themselves from civilian intelligence agencies in terms of internal organization, hierarchization, and external environment. In fact, they are much more hermetic and inward-looking than the civilian counterparts. The role of the Defence Minister is also more relevant with regard to the essential intelligence tasks.

The head of government is assisted by Minister–Coordinator for Special Services which occupies a special and prominent position in the Council of Ministers. The Office of Minister-Coordinator was established in

1997 with the purpose of fulfilling such tasks as supervision over the functioning of the special services, coordination and control of their activities and cooperation with internal security agencies as well as competent authorities and services from other states. In 2007, the new Prime Minister Donald Tusk, the head of liberal Civic Platform, initially had shifted control over the special services to his Chancellery but later decided to delegate this responsibility to Minister of Internal Affairs. Therefore, the special services were directly supervised by Interior Minister as coordinator appointed by and subdued to the Prime Minister and also head of an agency of government administration responsible for internal security and law enforcement and thereby active in criminal intelligence and civilian counterintelligence. Such a strict attachment of intelligence services to the Prime Minister was abolished after the 2015 elections. Minister-Coordinator for Special Services was reconstituted as a member of the cabinet fulfilling tasks allocated by the Prime Minister and acting on behalf of the head of government as coordinator and supervisor of the special services.

Apart from the Office of Minister-Coordinator for Special Services, the Prime Minister and the Council of Ministers (the government) is assisted by the Board for Special Services. It is a consultative body entitled to give opinion and advice on matters concerning the planning, supervision and coordination of operations of the special services and of activities performed by the Police, Border Guard, Military Gendarmerie, Customs and other relevant institutions protecting the state's security. The Board is chaired by the Prime Minister and consists of the Secretary and the members who are Ministers of Defence, Internal Affairs, Foreign Affairs, Finance as well as the Head of the National Security Bureau and – if appropriate – Minister-Coordinator for Special Services. Meetings of the Board may be attended by the heads of the five special services as well as the Chairperson of the Parliamentary Committee for Special Services. In extraordinary circumstances the President may delegate his representative to a meeting of the Board.

The post-2015 developments in the intelligence community and the project of a "big reform"

The new government, headed by Beata Szydło but formed under heavy influence from Jarosław Kaczyński, the Chairman of the Law and Justice party, was composed of his staunch followers advocating uncompromised change in domestic politics as well as firm promotion of the national interest abroad.

One of them, Mariusz Kamiński, was nominated to the re-established post of Minister–Coordinator for Special Services. During the earlier short period of PiS's rule (2005-2007), he was an originator of the idea of establishing a special anti-corruption service. Having established the Central Anti-Corruption Bureau, Kamiński was appointed the first head and held this post until 2009 when he was dismissed on the charge of misconduct and abuse of his powers with regard to investigation into one of potential corruption plots (the so-called Land Affair). Next he was sentenced to three years in prison and banned from performing public functions for ten years.[17] He launched an appeal and in the meantime his party PiS won presidential and parliamentary elections. Soon after having been sworn as the President of Poland, Andrzej Duda pardoned Kamiński which provoked a stormy reaction of many lawyers claiming that act unlawful and the liberal opposition accusing the president of cronyism. The reason was that Kamiński's appeal was still with the appropriate court. Later on, Poland's Supreme Court ruled that the pardon was premature.

Notwithstanding these reservations, concerning particularly security clearance and access to classified documents[18], Minister-Coordinator Kamiński energetically started to perform his duties. He strengthened the Central Anti-Corruption Bureau in order to reduce tax fraud and evasion and thereby contribute to increased budgetary incomes required to finance costly social programs launched by the Szydło government. He also took up the task of preparing a "big reform" of the special services. The concept of reform emerged already before 2015. The former liberal government outlined a plan of consolidation of intelligence services under a single new ministry. Oversight would have been executed by a special governmental committee of state security. The Internal Security Agency (ABW) would have lost its law-enforcement competencies and converted into a classical counterintelligence service responsible to Minister for Internal Affairs. After the change in power, PiS revived a blueprint which had been prepared during the earlier period of its rule (2005-2007). It also entailed consolidation of intelligence services

[17] "Poland's Jailed Anti-Corruption Boss Hails 'Justice and Fairness', as President Side-steps Court Procedure to Pardon Him" *Inside-Poland.com*, 19 November 2015, accessed 15 September 2017 at http://inside-poland.com/t/polands-jailed-anti-corruption-boss-hails-justice-and-fairness-as-president-side-steps-court-procedure-to-pardon-him/.

[18] The Polish Law on the Protection of Classified Information stipulates in Art. 30.2. That the person who has been sentenced by final judgement to imprisonment for an intentional offense prosecuted by public accusation or for a deliberate fiscal offense may not be granted security clearance.

under a separate ministry. However, the influential Defence Minister Antoni Macierewicz was hesitant toward losing his control over military intelligence and counterintelligence. In November 2016 the media informed that Minister–Coordinator for Special Services had a ready-made proposal for reform. It included the establishing of a new Ministry for State Protection which would encompass all civilian intelligence services. Therefore, they would no longer be subordinated directly to the Prime Minister and their personnel would be significantly reduced.[19] However, no official draft was presented and several months later, in July 2017, the issue of reform reappeared in new circumstances.

Following the presidential veto over judicial reform, Jarosław Kaczyński gave an interview in July 2017 to the main conservative Catholic media outlet TV Trwam heralding an intention of launching new "big reforms", amongst them one concerning special services. Earlier, the media disclosed central tenets of a draft law on the National Security Agency prepared by Minister-Coordinator Kamiński. The new service will integrate the civilian intelligence services: ABW and AW and have expanded competencies with regard to surveillance, interception of communication, data mining, counterterrorism and all "threats to national security". A new Ministry of National Security will be established with the aim of controlling, overseeing and coordinating all special services, including the Central Anti-Corruption Bureau and both military intelligence agencies. Although the latter will keep falling within the remit of Defence Minister, the new Minister for National Security will be authorized to set guidelines as well as control and coordinate their activities. Political control over the Ministry of National Security also will undergo deep changes. The Board for Special Services will be replaced by a Board of the Chiefs of Special Services composed by the heads of four intelligence institutions chaired by Minister of National Security. Representatives of the president and prime minister **may** be invited to the meetings of the Board. Moreover, National Security Minister will have the right to request from the members of the Council of Ministers and other governmental bodies any information indispensable for the matters of national security.[20]

---

[19] "ABW i Agencja Wywiadu w jednym superresorcie? Minister Kamiński chce wielkiej reformy służb specjalnych" *Dziennik Gazeta Prawna*, 22 November 2016, accessed 14 September 2017 at http://forsal.pl/artykuly/994934,ministerstwo-ochrony-panstwa-abw-i-agencja-wywiadu-sluzby-specjalne-reforma-kaminski.html.

[20] "Superminister od bezpieczeństwa" *Onet.pl*, 12 June 2017, accessed 14 September 2017 at http://wiadomosci.onet.pl/tylko-w-onecie/superminister-od-bezpieczenstwa/v7k36cl.

Meanwhile, the Internal Security Agency (ABW) underwent reorganization in mid-2017. Regional representations were reduced to only five and "external departments" replaced the resting representations. This entailed significant personal reshuffling aiming to dismiss officers with professional record tracing back to the Communist period. Although details were not announced to the public, budgetary plans point to a relatively wide scope of changes in the personnel. According to a well-informed "Rzeczpospolita" daily, the changes resulted in resignation from service of many experienced officers, especially from counterintelligence division.[21]

So far, the intelligence community was based on five agencies – special services. A draft law on the State Protection Service (PSO) suggests the emergence of yet another special service. PSO is intended to replace the Government Protection Bureau (BOR) - a uniformed and armed service with the task of protecting top government officials and key state buildings. PSO is endowed with additional competencies, going far beyond the routine activities of close executive protection and escort of top public officials and main state facilities. Its tasks include detection, identification and prevention of crime through investigation and information gathering. Specifically, PSO officers are responsible for identifying and analysing threats to protected persons and properties. For this purpose, they can introduce operational control in order to gather criminal intelligence through surveillance, eavesdropping and interception of communications as well as processing and storing data acquired from IT systems, including personal data, and biometric traits as well as genetic data amongst them. PSO is headed by the commander whose status is comparable to that of the chiefs of civilian intelligence services.

The post-2015 political transformation under the heading of "good change" entailed massive personal movements. They resulted partially from disagreements with the new authorities over the course of reforms, and were particularly evident in the Armed Forces, partially from ideological and political motivations behind PiS's strategy. They could also be observed in the special services, although had less to do with dissent among the personnel; rather, they were imposed by the new authorities as an element of reconstruction of the intelligence community and "cleaning of deposits" left by former Communist officers. The latter objective corresponded with the conspiracy-like "system theory" heralded by the opponents of the political pacts concluded by Solidarity-led opposition with the Communist authorities

[21] "Wielkie czyszczenie w ABW" *Rzeczpospolita*, 28 September 2017, accessed 29 September 2017 at http://archiwum.rp.pl/artykul/1354418-Wielkie-czyszczenie-w-ABW.html.

in 1989. Its main exponent, Andrzej Zybertowicz, a professor of sociology and the Nicolaus Copernicus University in Toruń and adviser to leading PiS politicians, maintained that the former communist secret services controlled the transition from Communism and kept their influence on the post-1989 transformation. Economy, security and law enforcement were the main domains of their hold. They were tolerated by the consequent democratic governments because either of their opportunism and fear of vengeance or by direct involvement of the protagonist of democratic transformation in collaboration with the former Communist services, including the famous leader of Solidarity, Lech Wałęsa. This thesis was resolutely advanced by the current Defence Minister Antoni Macierewicz, a representative of the national-Catholic wing of the right sector who strove towards a systemic exposition of the former Communist assets in the state institutions. He has been a leading advocate of the conspiracy theory claiming that the tragedy in Smolensk in April 2010[22] was orchestrated by Russian secret services in the passive attitude of Polish intelligence and counterintelligence agencies.

Conclusions: Intelligence and Poland's security dilemmas of a frontline state

Geopolitically, Poland's traditional position between Germany and Russia escalates dilemmas of cooperation and conflict. Germany has turned into Poland's biggest and most important economic and political partner, whereas Russia, after the annexation of Crimea and open interference in Ukraine, has been considered to be the biggest threat to stability in Europe. It was underlined in the Defense Concept of the Republic of Poland that "Russia is ready to destabilize the internal order of other states and to question their territorial integrity by openly violating international law. Russia's actions are often camouflaged and conducted below the threshold of an armed conflict. [...] Russia is also likely to provoke proxy wars in various parts of the world in order to exert pressure on the Western countries. [...] This policy is highly coordinated with the operations of Russia's special services, including the deployment of such instruments as disinformation campaigns against other countries."[23] For now, the priority

[22]The presidential airplane with top officials on board, including President Lech Kaczyński and his wife, crashed near the Russian city of Smolensk descending in extremely hard weather conditions. The Polish delegation travelled to mark the 70th anniversary of the massacre in Katyn, where the Soviet secret police NKVD slaughtered 20,000 Polish officers.

[23] *Koncepcja obronna Reczypospolitej Polskiej. The Strategic Concept of the Republic of Poland*, Ministry of National Defense, May 2017, p. 24.

for the secret services, particularly ABW and CBA, has been investigation of cases of suspected offences or the most harmful for the national interest, especially in finance and economic management, activities of the former Civic Platform government.

Facing the increasingly complex security environment combining traditional pressure from the historical enemy in the East and new technology-driven threats in cyberspace, the Polish intelligence community must undergo substantive adjustment in order to cope effectively with constant challenges and tasks. Recent changes did entail reshaping and internal reorganization of agencies, services and units responsible for intelligence and counterintelligence, though they have not contributed yet to a higher effectiveness. Rather, they reflect the characteristic traits of the ruling party: politicization, ideologically motivated human resources management, double standards in democratic governance (de-communization, protection of fundamental rights, judicial oversight, public communication etc.), historical view on the current complex security environment, weakened cooperation with external partners, especially in the EU. A long-announced "big reform" of the special services seems to consolidate such model of the Polish intelligence community which would probably go more obsolete and dysfunctional with regard to Poland's national interests.

References:

1. "ABW i Agencja Wywiadu w jednym superresorcie? Minister Kamiński chce wielkiej reformy służb specjalnych" *Dziennik Gazeta Prawna*, 22 November 2016, accessed 14 September 2017 at http://forsal.pl/artykuly/994934,ministerstwo-ochrony-panstwa-abw-i-agencja-wywiadu-sluzby-specjalne-reforma-kaminski.html.

2. Dymek, Jakub, (2016), "Poland's Rightward Turn" *Dissent*, Vol. 63, No. 2, 2016, pp. 123-127.

3. "Emmanuel Macron called 'arrogant' and 'inexperienced' by Polish prime minister Beata Szydlo in worker spat" *The Telegraph*, 25 August 2017, accessed 28 August 2017 at http://www.telegraph.co.uk/news/2017/08/25/emmanuel-macron-called-arrogant-inexperienced-polish-prime-minister/.

4. Geostrategic Insights into the Joint Polish-Croatian "Three Seas Initiative", accessed 14 September 2017 at https://www.globalresearch.ca/geostrategic-insights-into-the-joint-polish-croatian-three-seas-initiative/5598048

5. Gruszczak, Artur, (2015), "Poland: A Skillfull Player", in Eleanor E. Zeff, Ellen B. Pirro (eds), *The European Union and the member states* (Boulder, CO – London: Lynne Rienner Publishers, 2015, 3rd ed.), pp. 259-278.

6. Gruszczak, Artur, (2016),"Poland: The Special Services Since the Independence", in Bob de Graaff, James M. Nyce (eds.), *Handbook of European Intelligence Cultures* (Lanham: Rowman & Littlefield, 2016), pp. 279-290;

7. Jasiewicz, Krzysztof, (2016), Agnieszka Jasiewicz-Betkiewicz, "Poland" *European Journal of Political Research Political Data Yearbook* Vol. 55, 2016, pp. 204–215;

8. Karnowski, Jacek, (2016), "Europejska (kontr)rewolucja" *W Sieci*, 12-18 September.

9. Lefebvre, Stéphane, (2016), "Poland's Attempts to Develop a Democratic and Effective Intelligence System, Phase 1: 1989–1999" *International Journal of Intelligence and CounterIntelligence*, Vol. 29, No. 3, 2016, pp. 470-502.

10. Markowski, Radosław, (2016), "The Polish parliamentary election of 2015: a free and fair election that results in unfair political consequences" *West European Politics*, Vol. 39, No. 6, 2016, pp. 1311–1322.

11. Ministry of Foreign Affairs, Republic of Poland, *Polish Foreign Policy Strategy 2017-2021*, pp. 6-7, accessed 14 September 2017 at http://www.msz.gov.pl/resource/0c98c3b2-9c5d-4c42-8761-f7827134ee76:JCR.

12. "Obama Rebukes Poland's Right-Wing Government" *The New York Times*, 8 July 2016, accessed 28 August 2017 at https://www.nytimes.com/2016/07/09/world/europe/obama-poland-nato-summit.html.

13. Ordonnance du Vice-Président de la Cour, 27 juillet 2017, dans l'affaire C-441/17 R, accessed 28 July 2017 at http://curia.europa.eu/juris/document/document.jsf?text&docid=193373&pageIndex=0&doclang=FR&mode=req&dir&occ=first&part=1&cid=455841.

14. "Polish defence minister denies overstepping powers" *Radio Poland*, 9 May 2017, accessed 28 August 2017 at http://www.thenews.pl/1/9/Artykul/306113, Polish-defence-minister-denies-overstepping-powers.

15. "Right-Tilting Poland Welcomes Trump as Europe Watches Warily" *The New York Times*, 5 July 2017, accessed 28 August 2017 at https://www.nytimes.com/2017/07/05/world/europe/poland-trump-visit-g20.html.

16. *The Strategic Concept of the Republic of Poland*, Ministry of National Defense, May 2017.

17. Zalan, Eszter, (2017), "EU Commission sets red lines for Poland on Article 7", *EU Observer.com*, 26 July 2017, accessed 28 July 2017 at https://euobserver.com/political/138618.

18. Zwolski, Kamil, (2017), "Poland's Foreign-Policy Turn" *Survival*, Vol. 59, No. 4, pp. 172-173.

INTERCONNECTED IN PRACTICE AND INSULAR BY NATURE? THE INTERNATIONALISATION OF THE FRENCH INTELLIGENCE APPARATUS

Benjamin OUDET *

Abstract

In our contemporary security environment, intelligence cooperation is a strategic and vital resource shaping French strategic stature. The Bill passed in July 2015 after Paris terrorist attacks (Loi renseignement du 24 Juillet 2015) stated that with the protection of national interest, intelligence must support defence and diplomacy policies. We argue in the paper that the development of French intelligence cooperation is a response aiming at mitigating the uncertainty of the contemporary security environment. Intelligence cooperation has become a natural extension of French intelligence cycle and a means of influence. At the same time, we point out a paradox: While French intelligence services are highly interconnected and involved in numerous cooperation arrangements on a bilateral and multilateral basis, the lack of information available and academic analysis, its history and the French Strategic stature of "autonomy", suggest that the French community remains "insular" (Rovner 2013). The French intelligence community and especially its foreign intelligence services are among the most secretive in Europe regarding cooperation arrangements, and the French Intelligence Studies are still in a state of infancy. The French intelligence cooperation should be investigated through intelligence cooperation studies, international relations theories and the following criteria: 1. Strategic priorities and security environment; 2. Established partnerships. 3. Capabilities. French services incentives to foster cooperation are driven by the likelihood of a potential partner to share information or facilities, and whether the partner shares strategic orientations and faces a common threat.

Keywords: *Intelligence, practice, French, international intelligence cooperation*

Introduction

"For us, the cooperation is very easy and highly automatic through the Five-Eyes system. But for the French services, it is based on a comprehensive and pro-active strategy of partnerships, following strategic priorities. It is harder to

* Poitiers University, France

manage and sustain effectively". Interview with a Canadian intelligence officer, Paris, 2016.

Due to its secrecy and the French scholar's reluctance toward intelligence services, French intelligence 'machinery' remains critically under-studied comparing to its American and British counterparts. Nevertheless, French military doctrine (White Paper on Defence and Security, 2013) has promoted intelligence to the first rank of strategic function (knowledge and foreknowledge) before "deterrence", "protection", "prevention" and "intervention". The Bill passed in July 2015 after Paris terrorist attacks (Loi renseignement du 24 Juillet 2015) stated that with the protection of national interest, intelligence must support defence and diplomacy policies. Over the past ten years, France has experienced a process of rationalization, centralization, modernization of its intelligence apparatus to support strategic stature and fulfill its international commitments (Chopin 2017; Chopin & Oudet 2016). The 2008 constitutional review created a Parliamentary oversight body (Délégation Parlementaire au Renseignement), whose effects on international cooperation is yet to come but could be enforced soon. The process of normalization and centralization has engendered the creation of the Coordonateur national au Renseignement (CNR) and the constitution of a formal "community" composed of first cycle services: DGSE, DRM, DRSD (Ministry of Defence), DGSI (Ministry of Intérior), Tracfin and DNRED (Ministry of Budget). Plus, a second cycle composed of seven services (Ministry of Interior) in charge of "territorial intelligence".

French services have bilateral relations with hundreds of foreign services, and they may have several counterparts in some countries. For example, in 2013 the director general of the DGSE stated that his services work with more than 200 foreign partners. In 2013, following the "red-line" policy shared by Barack Obama and French President François Hollande, the DGSE released an intelligence analysis reporting biological attacks by the Syrian regime, indicating a sea change in the relationships between French society its intelligence services. Despite its high degree of interconnectedness with international networks of cooperation French intelligence has not received much attention from academics. The French intelligence cooperation should be investigated through intelligence cooperation studies, international relations theories and following criteria: 1. Strategic priorities and security environment; 2. Established partnerships. 3. Capabilities. After a brief reminder of intelligence cooperation conceptual framework, we would like to show that if the French services are very interconnected in practice, they remain insular culturally.

I. International intelligence cooperation: A conceptual framework

I.1. Response to the "new normal" of uncertainty

In the contemporary strategic environment, intelligence cooperation becomes more and more complex and critical for national and international security. This trend is related to four factors: 1. the growing number and intensity of threats, crises, and conflicts which require a reaction from national and international; 2. The increasing importance of precautionary approaches to security that focus on preventive, pre-emptive and anticipatory measures; 3. The need to access advanced technologies and sophisticated tools enabling massive information collecting, processing and disseminating, and knowledge sharing. 4. The opportunity for private, non-state actor or anti-state entities to widely apply intelligence tradecraft (Gruszczak 2016).

Academic literature usually distinguishes four factors fostering cooperation: 1. No one agency can do and know everything; 2. Developed countries are particularly attractive partners for less fortunate services that can trade human intelligence for the more sophisticated and expensive technical products to which they would not otherwise have access; 3. Ultimately, intelligence cooperation occurs when potential benefits are evident, and the cost or risk of that cooperation well understood; 4. Cooperation can encompass some form of influence and provide. Four factors impede collaboration: 1. The difference in threat perception; 2. The asymmetry in the balance of power between the two parties; 3. Ethical considerations; 4. National legal framework for data sharing and human rights (Aydinli et Tuzuner 2011; Hess 2003; Lander 2004; Lefebvre 2003; Richelson 1990; R. J. Aldrich 2003; R. Aldrich 2011).

I. 2. Intelligence cooperation: definition and taxonomy.

International intelligence cooperation "is the liaison or collaboration between state bodies from one or more countries, responsible for the collection, analysis and/or dissemination of intelligence for purposes including defence, national security and the prevention and detection of serious organized crime"(Born, Leigh, & Wills 2015). It encompasses five types of activities: 1. Information sharing; 2. covert operational cooperation; 3. hosting facilities and equipment; 4. training and capacity building; 5. providing hardware and software.

Scope and depth of cooperation can vary cooperation agreement, regular or one-shot meeting regarding one issue or one collection discipline or Task Force. In December 2015, France was committed within "Task Force Fraternité" aimed at investigating Brussels terrorist attacks. Seven operational

meetings were organized in France, Europol, and Belgium. Currently, two liaisons officers are in charge of intelligence sharing with Europol. The cooperation increased after the creation in January 2016 of "European Counter-terrorism Centre, ECTC" hosted by Europol. Plus, following the emergence of a standard European counter-terrorism policy French police and gendarmerie special forces units (GIGN and RAID) are part of group Atlas grouping special forces units from 26 countries of the Union.

Cooperation can have a bilateral (the deepest for the French community) and multi-lateral form at tactical, operational and strategic levels. For the French intelligence community, they are a strategic resource at the heart of national security policy and are included in Defence agreement signed by France and its counterparts. Moreover, it seems important to undermine an overused cliché: Contrary to what has been portrayed in the media in the days after dramatic events, cooperation has become a natural activity of French services, a natural daily activity aiming at completing the French intelligence cycle. French intelligence has long been internationalized though its counter-terrorism activities since the 1980's. Former head of DST (Direction de la surveillance du territoire) under the Ministry of interior reports in his Mémoirs that the domestic service was involved in more than fifty international cooperation arrangements at the end of the 1980's. The then Director of DGSE Bernard Bajolet stated in 2013: "We (DGSE) have a broad and extensive cooperation with foreign partners. DGSE has developed almost 200 partnerships, domestic and foreign services and technical agencies (...). Plus, we have partnerships with countries that could be regarded as adversaries. In matters of intelligence, everyone is partner and adversary at the same time. Some are more partners than an adversary, and conversely".

The statement highlights the defining features of French cooperation strategy. French intelligence services sustain relationships with countries considered as adversaries. In 2016, Patrick Calvar the then director of DGSI (domestic intelligence service) announced that its services cooperation with Russian services about Syrian-Iraqi Chechens channels. In sum, there is not friendly secret services and secret services of friendly states. The hypothesis here is that in a world of uncertainty regarding threats, sustaining intelligence cooperation is a strategic resource.

I. 3. From "need to know" to "need to share."

Over the past few years, intelligence cooperation between domestic and international counterparts has become a "new normal" in political discourse. In practice, this trend marks the shift from one logic to one another:

From the "need to know" and the "tyranny of stovepipes" inherited from the Cold War to the "need to share" and the absolute necessity to "connect the dots". Intelligence services have to reform their "age of Cold war" structures and adapt themselves to the the "age of Terror" environment (Treverton 2011). David Omand in his remarkable book "Securing the State" argued that: "The world of intelligence is no longer a zero-sum game" (Omand 2010). Nowadays, the efficiency of intelligence services is assessed through to their abilities to coordinate with their domestic and international counterparts and be fully involved in all sources national threat assessment. It was the idea behind the creation of the French Conseil National du Renseignement, CNR, in July 2008, triggering a process of centralization and normalization of intelligence within the Executive Branch (the weakest equivalent of American Director of National Intelligence, DNI).

The risk that the lack of intelligence sharing might be responsible for dramatic events (terrorism) and an "intelligence failure" has become unbearable for the western public opinions. This tendency explains never-ending debates in France toward "intelligence failures" where the intelligence services are progressively acknowledged as the "first line of defence" and subject to more and more public and academic discourses. On the other hand, intelligence inner logics and functions remain misunderstood explaining why, after dramatic events, public opinion suspect intelligence failures for reason of internecine feuds, and dysfunction between services at odds with each other. On the European level, a lack of intelligence sharing is suspected to be a mark of national selfishness and a defence of narrow national interest against a common threat. Against this background, it is worth noting that the intelligence realm is experiencing an exponential increase in its cooperation arrangements.

Meanwhile, some scholars have described a double-process of globalization reshaping intelligence affairs. One is the globalization *of* intelligence by the mushrooming of intelligence cooperation arrangements making the international web of cooperation denser and tighter. The other is a process of globalization *in* intelligence related to the transnational nature of contemporary threats intelligence service are facing (A. D. M. Svendsen 2009; Svendsen 2012; Svendsen 2012;) Plus, Europe is experiencing a process of regionalization of its intelligence activities by the strengthening and widening of bilateral cooperation amongst state (horizontal cooperation) and within Union's structures (vertical cooperation) such as Intcen, Europol, Satcen (Geospatial intelligence centre in Torrejon, Spain), Club of Berne-Counter Terrorism Group). France is at the heart of these developments after 2013 Snowden affairs when a consensus appeared among security apparatus that

the improvement of the all-sources collection capabilities to guaranty strategic autonomy was an absolute necessity. Moreover, French services while enforcing their European cooperation refused to open doors for a "European FBI" or "European CIA."

II. French intelligence cooperation stature

II. 1 Strategic priorities and security environment

Foreign counterparts acknowledged the French services for their highly secretive nature. Joshua Rovner argued in 2013 that the French community is distinguishable by its "insular nature." The hypothesis marks a paradox regarding the highly interconnected French community in bilateral and multilateral relationships in Europe and the world. Thus, French services incentives to foster cooperation might be driven by the likelihood of a potential partner to share information, whether the partner shares strategic orientations and face a common threat. French services proclivity to commit themselves in cooperation depends on partner's capacities and competence and if the partner shares the French strategic orientations. What is remarkable with the French situation is that counter-terrorism activities seem to be considered out the scope of national sovereignty. The "need to share" is so high in counter-terrorism affairs that French services share almost 95% of their information, according to a senior representative of DGSE (Direction générale de la sécurité extérieure).

Therefore, French cooperation are experiencing a process of enlargement and deepening. With the autonomy of decision-making, intelligence is also a factor of influence within international organizations (EU, ONU-peacekeeping operations, NATO) and with assistance provided to countries structuring their intelligence apparatus (French-speaking Africa). One of the questions is the standardization of French intelligence cooperation since the reintegration of NATO command in 2008 and despite the refusal of the United States to integrate France into the Five Eyes system. These interactions are closely linked to the degree of trust between services. Patrick Calvar mentions the necessary rebuilding of confidence in non-espionage after 2013.

To put it in a nutshell, French cooperation strategy and the sustainment of all-source capabilities is driven by its incentives to maintain its autonomy of decision-making and means of influence. Nowadays, French intelligence partnerships are naturally part of French security and defence cooperation and were at the heart of discussions during Danish and Indian visits if French last June. Moreover, it is worth mentioning the French

commitment in peacekeeping operations by the Department of peacekeeping. With 940 troops contributing to eight PKOs, France is the second contributor to the members of the Security Council and the only one to deploy forces in support of the PKOs (Minusma-Barkhane; Operation Sangaris-Minusca; Operation Licorne / ONUCI). Moreover, France is the fifth contributor to the PKO budget (6.3%).

II. 2 Established partnerships: "France talks with everyone."

Intelligence cooperation is one of the components of Defense cooperation. This is the case of the Bill authorizing the agreement between the French and Jordanian governments, registered on 21 July 2017, propelled by the fight against Daesh. In 2017, an annual bilateral military cooperation plan formalized the various types of cooperation between the two countries. It provides targeted cooperation in the field of intelligence, air force, and Special Forces. The French Committee on Foreign Affairs, Defense and the Armed Forces states that "there is also cooperation in the field of military intelligence which, for reasons of confidentiality, is not included in this plan". This suggests that it is structured by other channels, such as DGSE or DRM (Direction du renseignement militaire).

Academic literature assumes that in democracy intelligence cooperation are closely related to foreign policy. Under no circumstances can cooperation become forms of counter-diplomacy or para-diplomacy. In May 2017, French Ambassador in Washington, Gérard Araud, declared to *National Review* that "Our military-intelligence-sharing cooperation with the Defence Department improved dramatically under former defence secretary Ash Carter. And Secretary Mattis has told us he is ready to go beyond the existing agreement. So for us, it has been critical. For instance, in the Sahel region (of Africa), it is millions of square kilometres and it is very, very tough in terms of intelligence. But the Americans are providing a lot of technical intelligence so that we can strike the terrorists when they cross the border from Libya into Tunisia, or from Mali into Niger. We have absolutely no complaints. We have no signals that things will be different under President Trump. And after the Paris attacks, the U.S. immediately volunteered to help us — to increase the exchange of intelligence — and on our side, at least, we are very satisfied". Then he was asked: "Do you believe, especially in the field of NSA signal intelligence, that the U.S. has helped save French lives in France?" He answered: "Really, I don't know — it's not because I am trying to underestimate what's happening. I am out of the intelligence channels" and added: "I receive a lot of notes coming from our intelligence services, but they

are notes on the political aspect. There are notes on topics where it's normal that I would be informed. The exchange between the NSA and France – I don't know why I would know. The principle we have in France is 'the need to know'". Assuming that M Araud is telling the truth, his two answers portrayed the French intelligence services role and positioning in French external action: *they support French diplomacy by collaborating with foreign counterparts, outside the official diplomatic channels*. Nevertheless, we cannot argue that this understanding is more than a hypothesis in the absence of information from others embassies with which to compare.

The internal reform of the community modifies the capacity of certain services to cooperate. Tracfin financial intelligence unit is now a member of the six services of the first circle of the French community. The expansion of the international cooperation is linked to his transfer to a specialized intelligence service in the financial field. Facing terrorist financing networks, Tracfin is developing its cooperation with Europol, which has hosted a secure exchange between European Financial Intelligence Units since January 2016. Tracfin is involved in the FATF (Financial Action Group created in 1989) and MONEYVAL and EGMONT in charge of the operational exchange of information between the 164 financial intelligence units existing in the world. In charge of the operational exchange of information between the 164 financial intelligence units existing in the world. Tracfin strives to ensure that operational exchanges take place in a short period. The unit has been developing and conducting bilateral cooperation with Belgium, Qatar and the Chinese services since 2015. Visits by delegations are also a reliable indicator of collaboration: 9 for the year 2016: Argentina, Egypt, Madagascar, United States, Ukraine, Belgium, Poland, Tunisia, Italy. Tracfin received in 2015 members of the US Congress and intervened before this institution. In 2016 France was at the initiative of a meeting day with their American counterpart. Tracfin received information from 99 CRF in 2016.

Additionally, alongside alliances and international organizations, there is an increasing interconnection between terrorist threat analysis centers such as the British Joint Terrorism Analysis Centre, the Danish Centre for Terrorism Analysis and the Coordination Centre in Germany. One of the challenges for French cooperation in the field of counter-terrorism will be the integration of the recently created CNCT (Counter-terrorism national centre under the supervision of the National Intelligence Coordination) and the articulation with the cooperation agreements already committed by the French services. The CNCT was created in June 2017, and it is too soon to speculate about its international cooperation and the shape it might take.

With the convergence of foreign policy priorities, cooperation at the strategic level is conditioned by the harmonization of perceptions of threats and the emergence of needs. This harmonization can be the result of analytical collaborations such as the one that took place in 2016 between the French external services (DGSE-Interaxions) and Canadian (CSIS) liaison services. DGSE is at the origins of the Think Tank "Interaxions". For the first time in its history, DGSE was part of a joint workshop conducted under the Chatham House rule, leading to the publication of a post-Daesh environment assessment. It considered by the DGSE as a significant step forward and a milestone in term international cooperation and synergy with French academics. During informal interviews I have had with former intelligence officers (DGSE), they confessed the cultural turn Interaxions represents for the French services, and the pride to see something that has never was done before! DGSE stated publicly that: "Interaxions is a privileged meeting place for interacting with all French and foreign academic, academic and professional expertise on the criterion of excellence. Everyone, through their experience and their specific approach, has one of the many keys to understand reality. It also allows external participants to benefit from the unique expertise of our analysts. Interaxions contributes the dialogue between the various actors. The events organized by Interaxions are open to the French intelligence community, our institutional partners and national correspondents and to the French ecosystem of strategic thinking, the contribution of Interaxions brings its. Some events are organized with our foreign counterparts". It is worth mentioning that, alongside their counterparts, French domestic services are involved in the process of internationalization. The French DGSI (Délégation générale à la sécurité extérieure) has a significant territorial network. It also has a large number of posts (the number remain classified) outside the International Co-operation Directorate of the Directorate General of the National Police. The Directorate of International Cooperation (DCI) is the first joint directorate between the National Police and the National Gendarmerie, which brings together the two internal security forces. It brings together police officers and gendarmes who work, side by side and in concert, to the international police cooperation set up by the State to better protect its citizens and its interests. Created on 1 September 2010, it has been fully operational since 1 January 2011. The various threats, such as terrorism, drug trafficking or cybercrime, originate outside our borders. Countering these threats requires close cooperation between countries. The network of Internal Security Attachés (ASI), made up of 250 police and gendarmes deployed in 93 embassies and covering 156 countries, is a sure bet. The creation of the DCI is in line with the general policy review. Indeed, it reduces costs and improves performance by

bringing together, in a single structure, the major players in international cooperation. It also makes it possible to draw all the consequences of the attachment of the National Gendarmerie to the Ministry of the Interior. Its missions are as follows: Implementation of the Ministry's international strategy and the implementation of France's foreign policy on internal security; To lead and coordinate the operational, technical and institutional cooperation of the National Police and Gendarmerie, except matters exclusively of intelligence services.

II.3 Capabilities: All source collection and modernization

France is one of the few European countries to have access to all civil and military intelligence and civilian intelligence services, including technical intelligence, including electronic intelligence (SIGINT). There can be no question of enumerating all the French capacities. To sum up, France has a unique human intelligence capability (Humint) in the Middle East, Maghreb, and West Africa. France is a privileged partner for all the security problems of the region, especially with the G5 Sahel countries with which France provide intelligence support regarding capabilities and training. In the same vein, the network of embassies (163), permanent representations (16) and its maritime area (2nd EEZ and 1st underwater zone) provide France with a worldwide presence and cooperation and collection points. Worth mentioning is that the strengthening of satellite capacities and the development of partnerships over the last few years. France has space cooperation with Germany (5 SAR LUPE satellites), Italy (4 satellites, Cosmo-Skymed), 2 Hélios satellites, 1 Pléiade satellite. While there are collecting and operating centers in six countries (France, Germany, Italy, Spain, Belgium, and Greece), CMOS de Creil remains the "system center" responsible for supplying foreign partners. The modernization process in Creil (40kms away from Paris) ("Intelligence campus") is accompanied by enhanced cooperation with European structures such as the Satcen, notably in the field of training and education. In 2016, as part of the National Imagery Analyst's Initial Course and the NATO International IMINT courses, two readings were given at the Creil Center. Cooperation with the Satcen also involves the liaison of a Seconded National Expert (SNE). They are seven for a total of 132 employees. Similarly, it should be noted that of the 41 visits and receptions of delegations to the Satcen in 2016, five concerned French representatives, more than any other member of the EU. Since the end of the 1990s the daily cooperation of intelligence SIGINT between France, Germany, and Holland. With Denmark and Belgium, it is estimated that a "Group of Five" is progressively structured around this information-gathering technique.

Conclusion

In the hypothesis of an "insular nature" of the French community, the proclivity to engage in cooperation depends on the characteristics (capacity, relevance, trust) of the partner potential. The likelihood of French cooperation will increase with a partner involved in the same strategic area of interest or facing the same threat, if the lack of cooperation can be perceived as national egoism and have consequences on domestic policy, if there are French and foreign forces engaged in the same theatre of operations or if the partner is a member of the Five Eyes. Finally, it must be stressed that all the impediments of cooperation cannot be overcome naturally in the "top-bottom" creation of dedicated international organizations. It requires trust and synergy between analysts from different countries (Palacios 2016). Building trust is a fundamental dimension of cooperation (Hoffman 2002; Igoe Walsh 2006; Cook, Hardin, & Levi 2007; Elhardt 2015 Van Milders 2017) that could be resolved by building a joint European intelligence culture through the harmonization of training processes and an epistemic community of analysts, but also by harmonizing perceptions of common threats at the strategic level and taking into account national foreign policies agendas.

References:

1. Aldrich, Richard. 2011. *Gchq: The Uncensored Story of Britain's Most Secret Intelligence Agency*. London: HarperPress.
2. Aldrich, Richard J. 2003. *The Hidden Hand*. Reprint. Woodstock: Overlook Books.
3. Aydinli, Ersel, et Musa Tuzuner. 2011. « Quantifying Intelligence Cooperation: The United States International Intelligence Behavior (USIIB) Dataset ». *Journal of Peace Research* 48 (5): 673-82.
4. Born, Hans, Ian Leigh, et Aidan Wills. 2015. « Making International Intelligence Cooperation Accountable ». Geneva DCAF.
5. Bajolet, Bernard, Audition devant la Commission de la défense nationale et des forces armés, 24 mars 2015, Compte rendu N°47.
6. Bajolet, Bernard, Audition devant la Commission d'enquête relative aux moyens mise en oeuvre par l'Etat pour lutter contre le terrorisme depuis le 7 janvier 2015, 25 mai 2016, Compte rendu N°29
7. Calvar Patrick, Audition devant la Commission de la défense nationale et des forces armées, 10 mai 2016, Compte rendu N°47.
8. Calvar Patrick, Audition devant la Commission d'enquête relative aux moyens mise en oeuvre par l'Etat pour lutter contre le terrorisme depuis le 7 janvier 2015, Compte rendu N°28

9. Chopin, Olivier. 2017. « Intelligence reform and the transformation of the state: the end of a French exception ». *Journal of Strategic Studies* 40 (4): 532-53.

10. Chopin, Olivier, et Benjamin Oudet. 2016. *Renseignement et sécurité*. Armand Colin.

11. Cook, Karen S., Professor Department of Politics Russell Hardin, et Professor Margaret Levi. 2007. *Cooperation Without Trust?* New York: Russell Sage Foundation Publications.

12. Elhardt, Christoph. 2015. « The causal nexus between trust, institutions and cooperation in international relations ». *Journal of Trust Research* 5 (1): 55-77.

13. Gruszczak, Artur. 2016. *Intelligence Security in the European Union: Building a Strategic Intelligence Community*. 1st ed. 2016. London: Palgrave Macmillan.

14. Hess, Sigurd. 2003. « Intelligence Cooperation in Europe 1990 to the Present ». *Journal of Intelligence History* 3 (1): 61-68.

15. Hoffman, Aaron M. 2002. « A Conceptualization of Trust in International Relations ». *European Journal of International Relations* 8 (3): 375-401..

16. Igoe Walsh, James. 2006. « Intelligence-Sharing in the European Union: Institutions Are Not Enough ». *JCMS: Journal of Common Market Studies* 44 (3): 625-43.

17. Lander, Sir Stephen. 2004. « International intelligence cooperation: an inside perspective ». *Cambridge Review of International Affairs* 17 (3): 481-93..

18. Lefebvre, Stéphane. 2003. « The Difficulties and Dilemmas of International Intelligence Cooperation ». *International Journal of Intelligence and CounterIntelligence* 16 (4): 527-42.

19. Omand, David. 2014. *Securing the State*. Reprint. Oxford University Press, USA. Benjamin Oudet. IKS Conference. Bucharest, Romania 13 October 2017

20. Palacios, José-Miguel. 2016. « Intelligence Analysis Training: A European Perspective ». *The International Journal of Intelligence, Security, and Public Affairs* 18 (1): 34-56.

21. Richelson, Jeffrey T. 1990. « The calculus of intelligence cooperation ». *International Journal of Intelligence and CounterIntelligence* 4 (3): 307-23.

22. Rovner, Joshua. 2013. « NATO Intelligence Sharng in the 21st Century ». Columbia School of International Public Affairs.

23. Svendsen, Adam D. M. 2009. « Connecting Intelligence and Theory: Intelligence Liaison and International Relations ». *Intelligence and National Security* 24 (5): 700-729.

24. ———. 2012. *[The Professionalization of Intelligence Cooperation: Fashioning Method Out of Mayhem]*. Palgrave MacMillan.

25. Svendsen, Adam Svendsen; Adam D. M. 2012. *Understanding the Globalization of Intelligence by Adam Svendsen*. Palgrave Macmillan.

26. Treverton, Gregory F. 2011. *Intelligence for an Age of Terror.* Reprint. Cambridge ; New York: Cambridge University Press.

27. Van Milders, Lucas. 2017. « Does Cooperation at the International Level Require Trust? » *E-International Relations*. Consulté le avril 21. http://www.e-ir.info/2012/04/29/does-cooperation-at-the-international-level-require-trust/.

SECURITY CULTURE AND PUBLIC DIPLOMACY

POLICIES FOR SUPPORTING INDIVIDUAL WELLBEING AND PROSPERITY: A CRUCIAL ASPECT OF HUMAN SECURITY

Ileana-Cinziana SURDU *

Abstract

Several aspects concerning human communities, societal development and the social environment converge into issues related to human security. This perspective offers the possibility of analysing human security in a broader approach than just violence related aspects.

A complete human security approach would include aspects of social reality: the economic situation, the status of the environment, the access to food and to health services, the political situation, the security of communities, and also individual and family related issues.

Difficulties related to the struggles which families encounter in trying to fulfil their family responsibilities, their job duties, and personal aspirations, all have an impact at micro and also at macro level. These issues can reflect on individuals, on their families, over the community and the society, as a whole, through the vulnerability of the families, the vulnerability of children, stress related issues, the continuous decline of the birth rates, a lower professional performance, lower professional aspirations etc. All these aspects, acting alone or together, may register a negative impact over the economy. Here is where work-life balance policies, intersected with actions related to the wellbeing and prosperity of individuals come into act to ensure the human security of citizens.

The paper analyses the policies for supporting the wellbeing and prosperity of individuals and families, and the policies for supporting the work-life balance of individuals and families, starting with a short incursion into the essential dimensions of human security, firstly established by the United Nations Development Program (UNDP) in 1994, through its Human Development Report (HDR). The study reflects on economic security, as defined by the HDR, in relation to the human security concerned with the daily life aspects of individuals: family, community and jobs, analysed through work-life balance policies. The study analyses the European and on the Romanian normative framework regarding work-life balance, as determinant factors of human security.

The analysis reflects on the programs and actions implemented at European and at national level in relation to aspects that define wellbeing and prosperity of individuals and families, translated through work-life balance policies and norms, all

* PhD student, University of Bucharest, The Faculty of Sociology and Social Work, Doctoral School of Sociology - ileana.cinziana.surdu@gmail.com; ileana.surdu@sas.unibuc.ro

regarded as good practices and as examples to follow in the process of ensuring human security.

Keywords*: human security, individual wellbeing, individual prosperity, work-life balance policies, economic security, the United Nations Development Program*

Argument: How do individual wellbeing and prosperity lead to human security?

"The world will never be secure from war if men and women have no security in their homes and in their jobs" (UNDP, 1994, p. 24). This is how the Human Development Report from 1994 summarizes the new forms of security for the 21st century, underlining the fact that the actions of the state for ensuring human security should not interfere in people's freedom to make choices regarding their personal and professional lives.

Human security is described as a right, which allows people to have access to opportunities of self-sustenance. Insecure people become a burden for society and the state. As such**, security policies aim at the securing of the individual's wellbeing and prosperity**, through the access to means of organizing one's life and of satisfying the daily needs: education, jobs, services etc. Human security is seen as a "critical ingredient of participatory development" (UNDP, 1994, p. 24), which integrates the freedom of people ensured through the different opportunities that allow them to be responsible and to manage their own lives.

Global human security arises as a global challenge, considering the weaknesses of national borders in front of threats. The global human security is discussed also through the impact of prosperity and poverty over the people's choices. Economic security and the access to crucial services (education, training, family related services), act as an important factor of human security, because the can lead to progress, wellbeing and prosperity. On the other hand, if poverty is the trend, people would start looking for better jobs, so migration would be the norm; the lack of opportunities could rise into violence, tensions, frustration, and illegal actions, which reflect over the population's wellbeing. (UNDP, 1994)

After the Cold Ward, the borders have started to open progressively, which led to a continuous linkage between internal and external security issues. The new reality, described through democracy and development at all levels, has resulted into a sense of freedom, prosperity and wellbeing for the citizens. (European Security Strategy, 2003)

Human security – approaches and applicability to social contexts

The dimensions of human security

The issue of human security has first been approached in 1994, by the United Nations, through its Human Development Report (HDR) (Gómez and Gasper, s. a.). The HDR accentuates two major aspects of human security: "the freedom from fear" and "the freedom from want", which are part of the human freedoms promoted by Franklin D, Roosevelt in 1941 (Gómez and Gasper, s. a, p. 2). The debate regarding the human rights continued, and in 1990 added the necessity to "live in dignity" (Gómez and Gasper, s. a, p. 2).

The idea of security of individuals has first been included in the Treaty of Westphalia, in 1648, which treats the people's rights and freedoms as being opposed to the state's security. Human security was first referred to in documents which stated the protection of human rights, like The United States Constitution (1787), The Declaration of the Rights of Man and of the Citizen (1789), the Bill of Rights (1791), or the funding documents of the Red Cross (1863), The Hague Conventions, The UN Charter etc. (Martin, s. a.)

Even though the concept of human security has been introduced by human rights policies, the first concept concentrates on the risk that may threaten the individuals' lives and wellbeing. While human rights are protected by legal instruments, human security uses mostly economic, and secondly political or military means. Human security aims to provide vital capacity and targets to prevent risks on a short term. (Martin, s. a.)

The Commission of Human Security (CHS), which was established In January 2011, treats human security given its role of guardian for the human freedoms and fulfilment, and has set the freedom to live in dignity as one of its three objectives. The concept of dignity comprises, in this situation, "the basic principles of democracy, the rule of law and human rights and freedoms" (Martin, s. a.).

The concept of "human security" has been assigned a generally accepted definition in 2012, by the United Nations General Assembly (GA). According to Gómez and Gasper (s. a.), the UN has expanded its focus from territorial security to individual security. The report accentuated the role of the member states in identifying and addressing the challenges of the people in relation to their living conditions, their values and their dignity as humans (Gómez and Gasper, s. a.). Human security represents a flexible aspect of the human life, which can be discussed in relation to several topics and contexts, as long as it foresees the understanding of the threats the people are confronted with (Gómez and Gasper, s. a.).

The HDR from 1994 has highlighted seven fields of human security: economic – risks related to the labor market, to income situation, or to social security; food – dealing with the threats derived from access to a healthy alimentation; health – understood by the access to health services; environmental – risks resulted from the environment degradation: personal – dealing with acts that have a personal physical or psychological impact; community – dealing with tensions and conflicts; and political – in relation to the human rights (UNDP, 1994).

Gómez and Gasper (s. a.) underline the fact that human security is not an issue only for the weak and vulnerable states, but it is an important aspects for all states and societies, and it should be tailored to the local and national threats and needs.

The HDR (UNDP, 1994, p. 22) underlines the need to recalibrate the thinking process "from nuclear security to human security". The report states that security has to enlarge its perspective, in order to include besides the state-related issues, also areas that refer directly to the people. Security of people was translated into "protection from the threat of disease, hunger, unemployment, crime, social conflict, political repression and environmental hazards" (UNDP, 1994, p. 22). After the Cold War, it became clear that many of these fears were produced within the state, and not between states, and for the people, the fears were mostly related to their daily lives, and not to national, regional or world catastrophes. "Human security is not concerned with weapons – it is a concerned with human life and dignity" (UNDP, 1994, p. 22). The report emphasizes the characteristics of human security in the 21st century in relation to the society:

1) universality – translated through the common threats to humans in any kind of state, in relation to the employment market, health, access to dangerous substances, the effects of industry over the environment, safety, or human rights;

2) interdependency – understood through the lack of borders when one nation's security is affected;

3) easier to ensure by early prevention – in relation to the costs of a counteraction;

4) people-cantered – defined through the direct relation between human security and the people's lives (UNDP, 1994, p. 22-23).

Human security has similar characteristics and impact over different types of societies, but the nations' fears differ: while rich nations fear the threat of violence, the access to dangerous substances, the spread of diseases, the negative impact of progress over the environment or the instability of the

labor market, poor nations fear the same issues and also more common threats that are present in their daily lives, such as hunger, diseases, or poverty. (UNDP, 1994, p. 24).

As a fundamental concept for analysing society and people's lives, human security can be better understood in its absence, but the Human Development Report from 1994 states that even though it can be described instinctively, it is better to use a common and concrete description. As such, the HDR describes human security as "safety from such chronic threats as hunger, disease and repression (…), protection from sudden and hurtful disruptions in the patterns of daily life – whether in homes, in jobs or in communities" (UNDP, 1994, p. 23).

As the above descriptions state, the HDR emphasizes for the 21st century the relevance of **human security** for people's lives, which **acts like a guardian for a safe and clear path in all the spheres of one's life: the family life, the professional career, or the societal life**.

The 1994 HDR asks that human security should not be defined as human development. The last refers to the extension of people's choices, while the first underlines the possibility to have choices, with no costs, and at any time. The two concepts and the effects of the component actions are also interdependent: while one is developing, so is the other, and when one is failing, the risks of failure is also present in the other. The history has confirmed this hypothesis, in periods of human deprivation, like poverty, famine, disease, ethnical conflicts etc., which lead to lack of power in any field, and which resulted into manifestations of violence. (UNDP, 1994, p. 23)

Human security is described through two major components: "freedom from fear and freedom from want" (UNDP, 1994, p. 24), aspects which are seen as interdependent when talking about world peace. The Cold War's end led to a reduction in the fear of nuclear threats, and to an increase of the fear of the results of global poverty and their impact over the world. This is where human security has gained a different meaning, and it started to address the people's security.

The economic security as human security factor

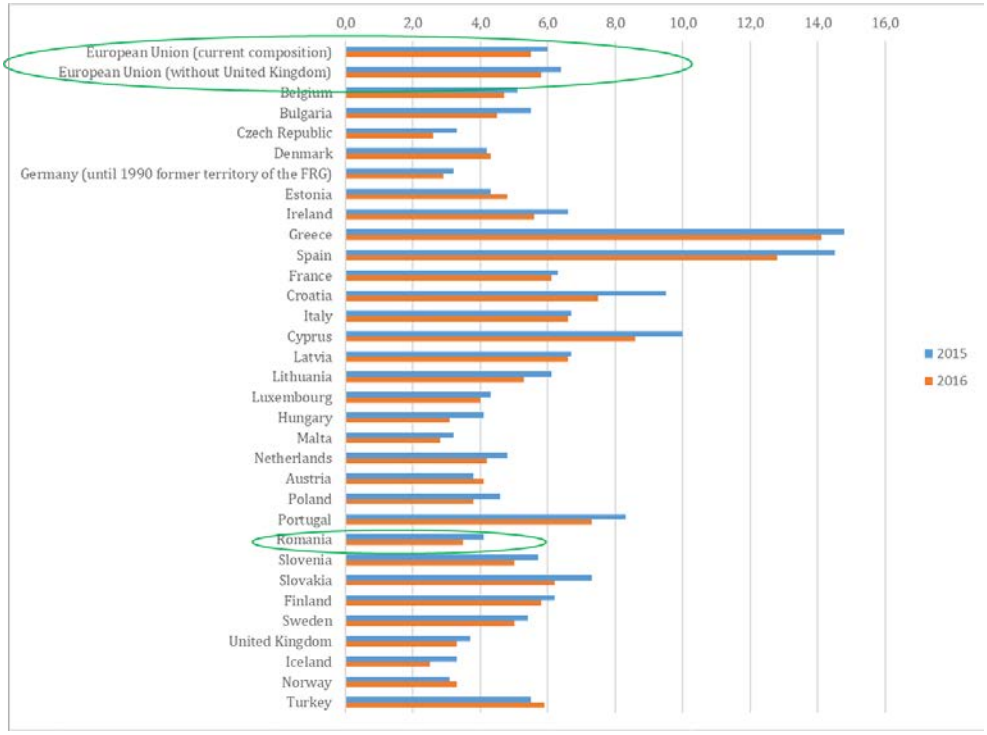
Human security from an economic perspective is defined in relation to the people's financial possibilities of sustaining themselves, at least as a basic level. The 1994 HDR states that only a quarter of the world's population is financially independent and, thus, economically secure (UNDP, 1994, p. 24).

Economic security is also differently perceived in relation to the state's situation, or in relation to demographic characteristics. Human security, from an economic point of view, for the rich nations, is discussed in relation to the instability of jobs and the lack of openings. The most vulnerable categories of people on the labour market are women, people from the rural areas and youngsters, and the feeling of being insecure is also high on people with part-time jobs. Developing countries usually present high unemployment rates, and the only resources for people in this situation are their families and communities, which also represent a fragile and on a short-term solution. The situation forces these people to accept any kind of job, regardless the payment, which can lead to other problems at personal level, like depression, dissatisfaction with their work, or lack of fulfilment in relation to their personal lives. Even self-employment is seen as a factor of a less secure economic state, in comparison to a monthly wage. Income insecurity describes the industrial societies also. The HDR from 1994 states that at the level of European Union, 28% of the work force gains less than have of the average income registered in their countries, and the United States registered a fall by 3% in earnings through the 1980s. Approximately 15% of the population from the United States and the European Union live under subsistence conditions. Segregated populations or disabled people, seen as human resources, are only a small part of the population that need training and access to jobs, in order to ensure economic security. (UNDP, 1994)

The government represents the final support-resource for the people to turn to, when facing poverty and economic insecurity. Having access to opportunities related to the labor market (education, training, jobs), ensures the economic security, and, as such, the human security (UNDP, 1994).

A short analysis over the statistical data regarding unemployment rates, show a decrease from 2015 to 2016 at European level and at the level of most of the states, except Denmark, Estonia, Austria, Norway and Turkey. Romania is on a descendant trajectory, also, in what concerns the annual average of unemployed people, out of the total population: 3.5% average in 2016, in comparison to an average of 4.1 in 2015. Even though the average of unemployment is lower than the average registered at European level, the data registered by Romania are considerably high.

Figure 1. Unemployment - annual average (% of total population), by year
Source: Eurostat



The data show a decrease in the average unemployment rate from 2015 to 2016 also concerning females and young people, under the age of 25, both at European and at national level. In 2016, the unemployment average in case of women decreased by 0.5%, while in case of youngsters it has decreased by 1%. The evolution describes an optimistic scenario for the employment rate, and, thus, for the human security status.

Figure 2. Unemployment by sex – females, annual average
(% of total population), by year
Source: Eurostat

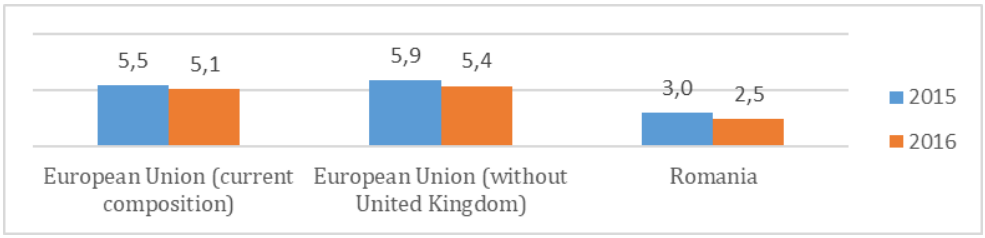
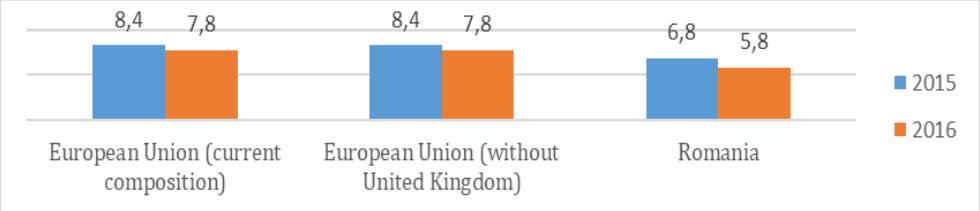


Figure 3. Unemployment by age – less than 25 years old, annual average (% of total population), by year
Source: Eurostat



A short incursion into the human security policies

According to the HDR (1994), the lack of human security worldwide requires the implementation of national and international human security policies. The policies developed during the past five decades, which targeted global security, regard security pacts and alliances in relation to physical attacks. The HDR requires a change of perspective and the implementation of policies for ensuring also the security of population (UNDP, 1994). Such policies would include:

- early warning indicators, used to describe the situation at national level and identify similarities, and, thus, potential crisis, which will help in preventing it;
- social integration actions, implemented firstly at national level, and afterwards at international level, by offering equal access to health and education services and to economic opportunities;
- ensuring access to work, by making sure of the availability of both opportunities and capabilities;
- access to human rights and political choices (UNDP, 1994).

As any other right or necessity, human security is tackled by dedicated institutions and through elaborated documents. Thus, The Commission on Human Security (CHS) published in 2003 "Human Security Now", which puts the bases of dignity of lives as one of the human security objective. The United Nations' efforts in assessing the concept of human security have been presented in the "A More Secure World" report, released in 2004, which treats human security in line with national security. In 2005, the three much discussed elements of human security – freedom from fear, freedom from want and freedom to live with dignity – have been stated as the base of the concept, through the report "In Larger Freedom: Towards Development, Security and Human Rights for All". The UN resolution 66/290 established the role of member states in identifying threats to human security, and highlighted the rights of vulnerable people to equal opportunities (Martin, s. a.). The European Security Strategy (2003, p. 2) emphasizes the security as a "precondition for development".

The Barcelona Report of the Study Group on Europe's Security Capabilities (2004) highlights the need for the European Union to address human security, as it directly involves the security of European citizens. The doctrine proposes seven principles of a human security policy:

1) "the primacy of human rights" – respecting the citizens' human rights equally;

2) "clear political authority" – accentuating the fact that human security must be managed by a capable political authority;

3) "multilateralism" – targeting the political and diplomatic actions, that must always be interconnected internationally;

4) "bottom-up approach" – the implemented actions must be decided in accordance to the people's needs;

5) "regional focus" – paying attention to regional clusters when addressing any kind of insecurities;

6) "the use of legal instruments" – as the rule in implementing any kind of action;

7) "the appropriate use of force" – only in cases when other solutions are not available. (The Barcelona Report of the Study Group on Europe's Security Capabilities (2004, p. 10-16)

The doctrine (2004) lists three reasons for which the European Union must integrate human security policies: from moral reasons in relation to the obligation to collaborate with all the member states when human security is at stake, for legal reasons, and for creating a common safe environment. Also, the doctrine for human security (2004) considers that these principles should be protected and implemented by a multinational civil-military "Human Security Response Force" (p. 17-19).

The Madrid Report of the Human Security Study Group (2007) discussed the evolution of European Security and Defence Policy (ESDP) through human security missions, both military and civilian.

The EU Global Security Strategy (2016) addresses the steps for including human security into European policies. It states that the priorities of the external actions regard the resilience to vulnerabilities, the prevention and response to conflicts in a comprehensive and integrated approach, seeking the instauration of a global order, which respects an international law, the human rights, and the progress.

Human security policies contribute to a new order of societies, which focus their actions on living freely, safely and in dignity. Such policies follow a bottom-up approach, starting from the needs of civilians, and addressing any type of threats towards human life. Human security policies focus on prevention rather than responses, and require the involvement of the civil society, of non-governmental groups and civilians. The process implies a

"comprehensive approach" in relation to the insecurities faced by the people, and also "multi-sectorial responses", with respect to the security issues, the development process, and the implementation of human rights. (Martin, s. a.)

Human security reflected in the work-life balance policies and framework

Policies that support the harmonization between the professional life and the family life

Vulnerable groups, like women, young people and rural areas locals, represent the population that urge the implementation of work-life balance policies, in order to eliminate the obstacles they (may) face in relation to the labour market. **After overcoming the age and distance issues, the women remain blocked in a circle that includes their career and their family life**, two important spheres of their lives which they have to juggle with, in order to maintain a balance. Work-life balance policies, in regard to the family life, can result in the efficient use of the women's professional aptitudes, in **the rise of productivity on the labour market, which can have a positive effect over the economy**. Overall, such policies could contribute to **achieving human security**. Also, according to the European Commission (2015), work-life balance policies can encourage men to get involved (more) in family responsibilities and give an opportunity to securing equality within the family.

The European Union foresees the equal distribution of household tasks between women and men, through its objective of employing 75% of women and men by 2020. The respective policies imply the collaboration of all member states, require the update of the European legal framework regarding maternity leave, the flexibility of the working hours, or the promotion of entrepreneurship. (European Commission, 2015).

In 2003, the first norms aiming to make the working schedule more flexible have been implemented through the labour code. Only in 2006 the balance between work life and family life has come into the focus of normative actions, through programs of assistance offered to working mothers with children under the age of two years old. (The Centre of Analysis and Social-Economic Innovation, 2014)

The most common policy of supporting the harmonization between family life and professional life is the indemnity offered to parents taking care of their new-born babies. This measure presents positive aspects, when looking at the bond created between the parent and the child, and also negative aspects in relation to the parent's professional activity. (Gagauz and Buciuceanu-Vrabie, 2011)

The 1994 HDR states that nations with slow population growth must benefit from family planning services and human development services. The

World Bank supports the implementation of cost-effective methods designed for offering this kind of services and estimates a number of 120 million of women from developing countries who would benefit of family planning services with a cost of 2 billion dollars per year. (UNDP, 1994, p. 34-35).

Baluta *et. al.* (2007, p. 7) propose for the Romanian framework a series of actions that may result with the desired balance, which could offer a security filling in relation to both the family and the job: the transfer of the maternity leave to the father, giving incentives for employers who offer child-care facilities, a flexible working program while on maternity leave for single-parent families. The National Agency for Equality between Women and Men (ANES) also proposes measures that target the conciliation between the family life and the working life: new facilities for taking care of children under the age of three, the promotion of gender equality within families, regarding the household task distribution, or the overlap of the working schedule with the one of the childcare institutions, like kindergartens or nurseries.

The Centre of Analysis and Social-Economic Innovation (2014) argues the role of a flexible working schedule in the achievement of the targeted equilibrium. The centre proposes the linking of payments to annual working hours, "flexi-time" – a situation in which people come to work and continue their working hours in a place of their choice, a simple flexible schedule, or part-time work. The centre also proposes the possibility of taking free days when the family responsibilities constitute a priority.

All these measures lead to positive results for the employee, who will become satisfied with the career and the family life, and will have a better financial situation, and also for the employer, who will register a higher productivity and more involved employees.

The European framework

The lack of services that can substitute the work within the household and in relation to the children, has led in most of the European states to a small share of women on the labour market, especially after giving birth. The European framework directed to the support of the work-life balance concerns the flexibility of the working schedule and the financial support dedicated to the children's development.

At the level of the European Union, the harmonization between the family and the professional life has first been introduced through the Lisbon Strategy (Leovardis and Nicolaescu, 2011). In 2015, the European Commission launched an initiative that establishes the need to update the legislative framework and the policies in regard to the family and the professional life, so that parents have the possibility to divide their time equitably, that couples

share their household responsibilities and that both parents can have the option to be active on the labour market. The initiative foresees the access to flexible working schedule, the access to parental leave for either one of the parents, the promotion of parental leave among fathers and the protection of parents that go through a reinsertion period after the parental leave. (The European Commission, 2015)

The European legislative framework protects women that are pregnant, breastfeeding mothers and women who just gave birth. The European Commission (a) has established a series of rights for these categories of women, like the right to not work on night shifts, the right to a 14-week paid leave before and after giving birth, the right to keep their jobs until they finish the parental leave and the right to a flexible program.

The Romanian framework

The Romanian legislative framework supports work-life balance and the equilibrium between family life and work life, through financial measures of protecting the maternity, resulted with payed parental leave, or financial incentives for families with children.

The Emergency Ordinance 111/2010 establishes a two-year parental leave and a three-year parental leave in case the child has a disability, and a 85% monthly indemnity reported to the net income from the last 12 months (within limited parameters) for the parent who takes the parental leave. Also, the other parent has the option to benefit of a month of parental leave within the first two years of the child's life, and from 5 to 15 working days of leave in the first two months of the baby's life (option conditioned by taking a childcare course). The ordonnance offers the possibility to dedicate time to the family in the first years of the child and also the possibility for the both parents to be involved.

In order to promote the earlier reinsertion on the labour market of the parents, the Romanian legislative framework, through the Government's Decision 449/2016, offers an incentive until the age of three years old of the child. This policy requires the efficient functioning of childcare services in relation to the parents' working program and to the parents' financial possibilities. Also, the parents have the option of interrupting or of prolonging the parental leave, supporting, this way, the harmonization of the professional activity and the family life of the new parents.

Also, the active mothers are protected through the Emergency Ordinance 96/2003, in relation to the work activity. The Emergency Ordonnance 105/2003, modified by the law 236/2008 stipulates the access to childcare subsidies for single-parent families in order to access childcare services, or to be able to sustain themselves, if the parent's wage is lower than the minimum wage.

Wellbeing and prosperity actions: good practices in ensuring human security

A study conducted by Baluta *et al.* (2007) directed to the conciliation of the family life and professional life, resulted with the declaration of parliamentary groups that these policies are a priority for the Romania's policies (with a mean of 9.1, where 10="very important"); trade unions do not agree with this, registering a 3.3 mean. In Romania there are four entities that are considered to be responsible with the work-life balance: The Commission for equal chances between women and men, The Commission for work and social protection, The Commission for budget, finances, banks and The Commission for health and family (Baluta *et. al.*, 2007).

European models of balancing the work and family life mainly describe the implementation of a flexible working schedule. According to ANES, Italy has introduced the practice of "time banks", which assume the recovery of overtime with free time; Italy has also implemented child-care services for children while parents are at work, the temporary replacement of employees who are on maternity leave, and training programs after the reinsertion on the labour market. Spain has also paid attention to policies for establishing a work-life balance, through the law 39/1999, which allows parents to feed their babies during the working hours and offers incentives to institutions that hire new personnel to fill the working time of new parents. France, on the other hand, offers incentives for education to parents in order to reinsert on the labour market, incentives for hiring a person to take care of the children under six years old, and through the Aubrey law (2000), France establishes a 35 hours week for institutions with more than 20 employees and special incentives for institutions which reduce the working hours with 10%. (ANES)

Germany has implemented a program which helps families to obtain a balance between the work life and the family life, by implementing personalized solutions. Also, Finland, is a country for whom the childcare and the parent's work-life balance are important. The local authorities offer the possibility for children to benefit of childcare services and food after the parents finish their parental leave, for an affordable monthly tax. (Gagauz and Buciuceanu-Vrabie, 2011)

A number of European countries have identified the possibility to ensure human security through economic security, having job-sharing as basic principle the. UNDP (1994) presents the case of Italian workplaces, which chose to reduce the work-week to four days and to cut the expenses, so that unemployed people could benefit of the working day and its costs. Germany implemented the four-day working-week also, in 1990, when BMW opted for a flexible program within one of its plants; because the flexibility of the program resulted with more gains, there was no need to cut off salaries in order to pay

the new workers. Volkswagen also introduced the four-week system, but with a 10% cut of the wage, not with the purpose of hiring new workers, but aiming to save the jobs of current workers, which it succeeded. The company Hewlett-Packard in France chose to adopt the four-day week program, which resulted into a 24 hours/7 days a week productivity, tripled production, 20% higher employment rate and unchanged wages. (UNDP, 1994)

The concept of job-sharing, presented through case studies by UNDP (1994), introduces a new perspective over human security in relation to the economic security. Many companies have adopted a flexible working program, with or without a cut off the salary, which gave the possibility to give economic stability and security to more employees. Some critics of job-sharing argue that this flexible program could have a positive impact over the private life, by having more free time at disposal, and to reducing unemployment, but on the other hand, it can have a negative impact to concentrating work into high-paid jobs and low-paid jobs (UNDP, 1994).

Conclusions – how human security reflects into wellbeing and prosperity status of the families

Human security policies focus the societies' actions towards living with a constant feeling of freedom, of safety and of dignity, always in connection with the people's needs. After the Cold War, people's fears moved from nuclear threats to global poverty threats, and the attention to the security of the state was directed to the security of individuals. The 21st century human security perspective targets the protection from disruptions in the daily life spheres of human beings: the family life, the professional life and the social environment. Human security is dependent on the economic factor, so one's financial stability positively correlates with his wellbeing and prosperity. Maintaining a distance from daily disruptions and also having the opportunity for financial independency, the individuals' security could be ensured in regards to their families and their jobs. A precondition of one's availability for being active and productive on the labour market is having the opportunity for work-life balance.

The Romanian legislative framework regarding the equilibrium between family life and work life, in case of families with children, mainly refers to the incentives offered to parents in order to have the possibility to dedicate themselves to the family during the child's first years of life, for both parents. On the other hand, the framework supports the balance between work life and family life through the option of earlier reinsertion on the labour market or of prolonging the parental leave, or even the shift of the leave between parents. The main policy that the employers implement, in relation to the work-life balance,

relates to the flexibility of the working program, which also offers the employees the opportunity to also take care or dedicate themselves to personal situations.

The option to work, in case of mothers, is dependent to the level of involvement of the father in the household and children responsibilities. European policies and legal framework that regulates the work-life balance, may contribute to the rise of birth rates and to the rise of the women's share on the labour market, and, thus, to the increase of productivity and qualification.

The main positive impact of the implementation of work-life balance policies could result in the increase of the rate of women's participation on the labour market, but also in a higher motivation of employees to work, in a higher level of productivity, and also in an economic increase, through the quality of work and through higher wages.

References:

1. A European Way of Security. *The Madrid Report of the Human Security Study Group comprising a Proposal and Background Report*. (8 November 2007). Madrid. Retrieved from http://eprints.lse.ac.uk/40207/1/A_European_Way_of_Security(author).pdf

2. *A Human Security Doctrine for Europe. The Barcelona Report of the Study Group on Europe's Security Capabilities*. (2004). Retrieved from http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/solana/040915CapBar.pdf

3. Baluta, O. (coord.). (2007). *Equal chances through the conciliation between family life and career*. Bucharest: MAIKO. The Centre for Curricular Development and Gender Studies: FILIA. Retrieved from http://centrulfilia.ro/publicatii/Volum-Sanse-Egale.pdf.

4. European Commission. (2015). *Roadmap. New start to address the challenges of work-life balance faced by working families*. Retrieved from http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_just_012_new_initiative_replacing_maternity_leave_directive_en.pdf.

5. *European Security Strategy. A Secure Europe in a Better World*. (12 December 2003). Brussels. Retrieved from https://europa.eu/globalstrategy/en/european-security-strategy-secure-europe-better-world

6. Eurostat. *Unemployment – LFS adjusted series: Unemployment by sex and age – annual average*. Retrieved from http://ec.europa.eu/eurostat/data/database

7. Gagauz, O., Buciuceanu-Vrabie, M. (2011). *The parental role and the professional role: opportunities of equilibrium for the contemporary woman*. Chisinau: The Academy of Science from The Republic of Moldova, The Institute for European Integration and Political Science – The Demographic Sector

8. Gómez, O.A. and Gasper, D. (s. a.). *Human Security. A Thematic Guidance Note for Regional and National Human Development Report Teams*. United Nations Development Programme. Human Development Report Office. Retrieved from http://hdr.undp.org/sites/default/files/human_security_guidance_note_r-nhdrs.pdf

9. *Law 236/31 October 2008 for changing the Emergency Ordonnance no. 105/2003 regarding the complementary family incentives and the sustaining incentives*

for the single-parent families. Retrieved from http://www.mmssf.ro/pub/imagemanager/images/file/Legislatie/LEGI/L236-2008.pdf.

10. Leovaridis, C., Nicolăescu, A. (2011). *The report between the professional life and private life. A EU's present preoccupation in the field of the labor market*. The Romanian Sociology Magazine. Year XXII, no. 1-2, p. 108-122. Bucharest. Retrieved from http://www.revistadesociologie.ro/pdf-uri/nr.1-2-2011/06-CLeovaridis.pdf.

11. Martin, M. (s. a.). *Human Security Course*. e-Learning platform. "Claim! - Citizens Network for Peace, Reconciliation and Human Security" - Project supported by the European Commission. Retrieved from http://humansecuritycourse.info/

12. The Center of Analysis and Social-Economic Innovation. (2014). *The reconciliation between family life and professional life*. Retrieved from http://www.femeia21.ro/images/Reconcilierea%20vietii%20de%20familie%20cu%20cea%20profesionala%20final.pdf.

13. *The Emergency Ordonnance 96/14 October 2003 regarding the protection of maternity at the working place*. Retrieved from www.mmuncii.ro/pub/imagemanager/images/file/Legislatie/ORDONANTE-DE-GUVERN/OUG96-2003.pdf.

14. *The Emergency Ordonnance no. 105/24 October 2003 regarding the complementary family incentives and the sustaining incentives for the single-parent families*. Retrieved from http://www.mmuncii.ro/pub/imagemanager/images/file/Legislatie/ORDONANTE-DE-GUVERN/OUG105-2003_act.pdf.

15. *The Emergency Ordonnance no. 111/8 December 2010 regarding the parental leave and the monthly incentives*. Retrieved from http://anes.gov.ro/wp-content/uploads/2017/09/10.-OUG-Nr-111-din-2010-privind-concediul-si-indemnizatia-lunara-pentru-cresterea-copiilor.pdf.

16. The European Commission (a). *Professional, private and family life*. Retrieved from http://ec.europa.eu/justice/gender-equality/rights/work-life-balance/index_en.htm.

17. The European Commission. (2015). *Roadmap. New start to address the challenges of work-life balance faced by working families*. Retrieved from http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_just_012_new_initiative_replacing_maternity_leave_directive_en.pdf.

18. The European Union. *Shared Vision, Common Action: A Stronger Europe. A Global Security Strategy for the European Union's Foreign and Security Policy*. (June 2016). Retrieved from https://eeas.europa.eu/headquarters/headquarters-homepage/17304/global-strategy-european-unions-foreign-and-security-policy-june-2016_en

19. The Ministry for Work and Social Justice. *The Decision 449/22 June 2016 for modifying and completing the methodological norms of application the Emergency Ordonnance 111/2010 regarding the parental leave and the monthly incentives approved by the Government's Decision 52/2011*. Retrieved from http://www.mmuncii.ro/j33/images/Documente/Legislatie/2016/HG449din2016_normeICC.pdf.

20. The National Agency for Equality between Women and Men (ANES). *The conciliation between family life and professional life*. Retrieved from http://www.mmuncii.ro/pub/imagemanager/images/file/Domenii/Egalitate%20de%20sanse/Brosura%20conciliere.pdf.

21. UNDP. (1994). *Human Development Report 1994*. New York: Oxford University Press. Retrieved from http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf

RETHINKING LEGAL FRAMEWORKS FOR INTELLIGENCE AGENCIES: RECONCILING THE STRUCTURE AND PROCESS OF INTELLIGENCE WITHIN THE LAW

Karen MOHAN *

Abstract

Intelligence has evolved organically in response to a rapidly changing security environment and currently involves a range of actors who partake in the intelligence process. This evolution for the most part has not been accompanied by appropriate legislative reform, which has created a serious gap between the law and the activities of the intelligence sector. There is currently no single national framework governing intelligence activities. This is due to the fact that there are a number of state and non-state actors carrying out intelligence work, including general intelligence, the police, the military, financial institutions, the private sector and civilians. These actors are all subject to different regulations, leading to a potential breakdown in the intelligence process. This blurring of boundaries has also raised serious concerns over public policy and civil liberties. In order to address this issue, both the structure and function of Intelligence should be taken in to account when proposing law reform, which ensures that all actors are sufficiently covered by a common set of rules and regulations, which will not only ensure that all actors engaged in the process are sufficiently regulated, but will also ensure that the intelligence process is working effectively.

Keywords: *Intelligence Actors, Intelligence Process, Intelligence Structure, National Legal Frameworks, Human Rights, Effectiveness*

Introduction

In recent years the global security environment has experienced significant change. In an effort to combat and contain security threats, national security policies across the globe continue to evolve and become tougher. As part of this evolution, Intelligence activities are now carried out by a range of actors, including non-state actors, such as private companies and individuals. In addition, the lines between state actors have become

*Marie Sklodowska-Curie Research Fellow/PhD candidate, Rijksuniversiteit Groningen, Faculty of Law, k.p.mohan@step-rug.nl

blurred, with a trend towards increasing integration between the police and Intelligence services.

As a result of the vast number of actors involved in intelligence, national legal frameworks have become increasingly complex, with different rules and regulations governing different actors involved in the intelligence process. In some circumstances, no appropriate legal frameworks exist at all. This not only complicates attempts to initiate legislative reform, but also potentially creates fragmentation within the process itself, as well as creating a disconnect between Intelligence as an organisational structure and the process of Intelligence. In the absence of appropriate legal reform in this area which clarifies the roles and functions of different actors involved in the Intelligence process, it is likely that the law will continues to undermine rather than promote organisational effectiveness, as well as the protection of human rights.

1. The Use of State and Non-State Actors in the Intelligence Process

There are a number of different legislative frameworks governing the activities of actors involved in the intelligence process.[1] This is due to a range of different state and non-state actors currently engaged in intelligence work, including general intelligence, the military, law enforcement, private entities and private persons.[2] In the UK, the use of actors, including healthcare professionals and school teachers, has been heavily criticized. The UK, as part of the 'prevent' strand of its counter-terrorism strategy (CONTEST), has 'laid down a vast infrastructure' of surveillance through institutions and communities, including schools, the National Health Service (NHS) and nurseries, in order to map the Muslim population in an effort to prevent radicalisation.[3] According to Elshimi, Intelligence should be left to the professionals and not delegated to teachers and health care workers. He points out that this is not only bad practice, but also counterproductive because of the risks of producing poor intelligence. [4] The use of private sector contractors has also been a subject of some concern. Although Intelligence was traditionally a function of government institutions, strategic intelligence

[1] Peter Roudick "Foreign Intelligence Gathering Laws" *The Law Library of Congress*, 2006, p. 1
[2] Ibid., p. 1
[3] M S Elshimi, *De-Radicalisation in the UK Prevent Strategy: Security, Identity and Religion* (Routledge, 2017)
[4] Ibid.

is increasingly been used by the private sector. [5] For example, the private sector now uses open source information in a fashion similar to that of government intelligence agencies. [6] In addition to private actors, attempts to integrate the activities of state actors, as well as the growing trend towards the establishment of fusion centres has raised serious questions both with respect to the protection of human rights and the effectiveness of such operations.

The core function of Intelligence agencies is the 'collection, analysis and dissemination' of information for the purposes of protecting national security. According to a 2010 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering Terrorism', many countries limit the functions of their intelligence agencies to carrying out this core function, thus preventing them from becoming involved in other security functions, which are already undertaken by other state actors. This, according to the report, is a matter of good practice and should be clearly defined in legislation.[7]

However, a number of countries now have a mixture of 'national security intelligence 'and 'policing intelligence' contexts. Walsh points out that post 9/11, what fits in to the category of 'national security intelligence' and that of 'policing intelligence' has blurred significantly. When examining countries which make up the 'five eyes' network, Walsh found that attempts have been made to harmonise certain aspects of their core intelligence activities, including collection and the production of intelligence products.[8] Walsh argues that intelligence frameworks, which include the use of non-intelligence staff, must ensure that these actors are sufficiently engaged through all stages of the implementation of these frameworks at agency and local level, through a 'well-crafted intelligence doctrine providing a common set of policies'.[9] Lutterbeck points out that the convergence of intelligence and police services has led to both the 'policisation' of intelligence services and 'intelligence – isation' of police work including the use of sophisticated

---

[5] Lisa Krizan "Intelligence Essentials for Everyone" *Joint Military Intelligence College Washington D.C.*, Occasional Paper no. 6, 1999, p. 7
[6] Ibid., p.10
[7] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/14/46
[8] Patrick F Walsh "Building Better Intelligence Frameworks Through Effective Governance" *International Journal of Intelligence and Counter Intelligence*, Vol. 28, No.1, 2005, p. 126
[9] Ibid., p.132

surveillance techniques, which were originally intended for intelligence use.[10] This has resulted in the boundaries between actors becoming increasingly blurred, overlapping with one another, or in some circumstances disappearing entirely. This shift towards more intrusive policing and the involvement of intelligence services in crime control and policing, Lutterbeck points out, is not a neutral development, as the absence of such separations are often associated with authoritarian or repressive regimes, raising difficult ethical and political questions. [11]

1.1. Outsourcing Intelligence to Private Actors

Given the lack of regulatory controls, one of the biggest threats to civil liberties is likely to come from private agencies in the future.[12] A significant number of intelligence activities are now been outsourced to private companies. [13]According to the Ministry of Justice in the Netherlands, it has been estimated that the number of 'private entities' who now collect information is between 500 and 1000.[14] Hoogenboom points out that one of the implications of the growth of informal intelligence activities carried out by private actors including debt collectors, multinationals, information brokers and private security consultants, is that State agents can potentially outsource activities that they would otherwise not be allowed to carry out due to national regulatory control[15] because these private actors are generally not subject to judicial or parliamentary oversight. Chesterman also argues that the involvement of private companies in top level analysis is problematic because this analysis often forms the basis of public policy, raising questions about whether it's appropriate for the private sector to have this amount of influence on the Executive. [16] The abuse of sensitive information is also a concern, when 'a profit motive is inserted in to intelligence activities'. [17]

---

[10] Derek Lutterbeck "Blurring the Dividing Line: The Convergence of Internal and External Security in Western Europe" *European Security*, Vol. 14 No. 2, 2005, pp. 240–250
[11] Ales Zavrsnik "Blurring the Line between Law Enforcement and Intelligence: Sharpening the Gaze of Surveillance?" *Journal of Contemporary European Research,* Vol. 9, No. 1, 2013, pp. 181 - 202
[12] Ibid.
[13] Siobhan Martin "Spying in a Transparent World: Ethics and Intelligence in the 21st Century" *GPSC*, Geneva Papers, Vol. 19, No. 16, 2016, p.18
[14] Bob Hoogenboom "Grey Intelligence" *Springer*, Crime Law Soc Change, Vol. 45, 2006, p.380
[15] Ibid., p. 377
[16] Simon Chesterman "We Can't Spy … If We Can't Buy! :The Privatization of Intelligence and the Limits of Outsourcing ' Inherently Government Functions, *The European Journal of International Law*, Vol. 19, No. 5, 2008, p. 1057
[17] Ibid., p.1068

In some circumstances, such as the case of private contractors who carry out intelligence functions, the profitability of these companies rely entirely on carrying out security intelligence. In countries, such as the United States, where the outsourcing of Intelligence has become commonplace (already by 2005, private contractors received 70 percent of the US intelligence budget, totalling 42 billion dollars.[18]), it has been reported that almost one third of private intelligence contractors have top level security clearance[19]. In 2007, a US House Permanent Select Committee report expressed concern about the growing number of private contractors involved in intelligence activities, suggesting that some functions should remain inherently governmental. The report stated:

> *"Intelligence Community leaders do not have an adequate understanding of the size and composition of the contractor work force, a consistent and well-articulated method of assessing contractor performance, or strategies for managing a combined staff – contractor workforce. In addition, the Committee is concerned that the Intelligence Community does not have a clear definition of what functions are 'inherently governmental' and, as result, whether there are contractors performing inherently governmental functions."* [20]

The use of private intelligence contractors is problematic with respect to a number of issues, including the gathering of information by means that would otherwise be illegal and immunity from prosecution. Hoogenboom, uses the term 'grey intelligence', which is derived from research in to the blurring of boundaries between 'public and private security' in the UK, to describe the complex nature of the relationship which exists between the private sector and Intelligence, arguing that the public is often far too focused on the traditional structures of intelligence, such as MI5, MI6 and the CIA, whilst it should be more concerned about the grey area in which private intelligence corporations are now operating and the grey lines which separate state and private actors carrying out state functions.[21]

---

[18] Ibid., p. 1057
[19] Peter Gil "The Implications of Intelligence Practice Within and Beyond the State: An Analytical Model*, Journal of Regional Security*" Vol. 8, No. 2, 2013, pp.93-144
[20] House of Representatives Report on Intelligence Authorization Act for Fiscal Year 2008 (Permanent Select Committee on Intelligence, Report 110-131, Washington, DC, 7 May 2007) in Ibid.
[21] Ibid.,p.373

Martin points out that the leaking of over 200,000 classified documents by Edward Snowden in 2013 and revelations with regard to the outsourcing of operations and interrogations reveal the degree to which intelligence agencies have become dependent on private actors, who are not subject to the same regulatory frameworks or accountability mechanisms. In this regard, these actors need to be subjected to increased oversight and regulation.[22] Gill further argues that whilst much has happened in terms of legislating for state intelligence agencies, as well as providing appropriate oversight mechanisms in the past twenty to thirty years, the same has not happened with respect to private corporations carrying out intelligence activities. [23]

1.2. The Fading Line between State Actors: Integration between Intelligence and the Police in Europe

With respect to state actors, the disintegration of the boundary between the police and intelligence services has given rise to grave concerns. Whilst the police and intelligence services have traditionally been kept separate, with police services been subject to much stricter regulations, these two fields have seen increasing convergence due to the changing nature of threats. Close cooperation between the police and intelligence services can be seen in a number of countries across Europe. In France, for example, there is very strong cooperation between the Internal Intelligence service, the DST (Directorate of Territorial Surveillance) and the police in France. In addition, collaboration exists with respect to surveillance of migrant populations with the National Police (Direction Generale de la Police Nationale) under the auspices of the Ministry of the Interior, and the Gendarmerie (responsible for rural areas), which falls under the auspices of the Ministry of Defence. [24] The Anti-Terrorism Coordination Unit (Unité de Coordination de la Lutte Anti-Terroriste (UCLAT)) also coordinates interactions between internal intelligence and the police. In the Netherlands, although a strict separation exists between Intelligence and Law enforcement, a 2002 AIVD (General Intelligence and Security Service) report showed that police had made a number of arrests based on AIVD information. [25] The validity of this evidence

---

[22] Op. Cit. Siobhan Martin, p.1
[23] Op. Cit., Peter Gill, p.107
[24] Pater Chalk, William Rosenau "Confronting "the enemy within": security intelligence, the police, and counterterrorism in four democracies" *Rand*, 2004, p. 20
[25] Erik Akerboom "Counter-terrorism in the Netherlands. General Intelligence and Security Service of the Netherlands" *AIVD,* 2000, p.1

was questioned by the Rotterdam Regional court, but the court of appeal in The Hague found that the use of such evidence was lawful. [26] Traditionally in the UK, counter-terrorism functions were carried out by MI5, the anti-terrorism branch of the MPS and special branch officers within the police force. The role of special branch officers was to collect information for the purposes of legal proceedings. [27]In the past the sharing of 'intelligence data' between these three bodies was prohibited, but a number of interviews carried out in 2004 confirmed that this was no longer the case, and revealed that closer cooperation and intelligence sharing had between these organisations had now become commonplace. [28] . In 2000, the NIM (National Intelligence Model) was introduced which allowed the police to collect and process intelligence data.

Brown and Korff, point out that the police are increasingly seen as part of the 'full societal alliance' with respect to the implementation of state policies in Europe, which they argue has widened the area in which the state is now likely to act against those who have still not committed a crime. For example the UK's Anti-Terrorism, Crime and Security Act 2001 provides for the preventative detention of those suspected of potential terrorist activities. In addition, the definitions with respect to what constitutes the 'grounds of suspicion' in this regard have become increasingly vague. [29] A number of countries have now criminalised activities that 'support terrorism' , ''apologising for terrorism' or the possession of materials which may be used for terrorist activities, regardless of whether the intention was to use such materials for the purposes of terrorist acts or not. According to Brown and Korff, widening the powers of the police in such a manner, leaves the door open to penalising citizens for their political beliefs and clamping down on their right to free expression. Also, discriminatory practices are widespread, with individuals belonging to certain ethnic groups been regularly targeted.[30]

In addition, information sharing has become more commonplace. This has led to a degree of secrecy around where police interest in a particular

---

[26] Ibid., p. 4
[27] Martin Innes "Policing Uncertainty: Countering Terror through Community Intelligence and Democratic Policing" *AAPSS*, Vol. 605, May, 2006, p.6
[28] Martin Innes, James W E Sheptycki "From Detection to Disruption: Some Consequences of Intelligence-led crime control in the UK" *International Criminal Justice Review,* Vol. 14. 2004, pp.1-14 in Ibid.
[29] Ian Brown, Douw Korff, 2009. Terrorism and the Proportionality of Internet Surveillance*, European Journal of Criminology*, Vol. 6, No. 2, p.126
[30] Ibid., p. 127

suspect has originated from, in addition to how evidence against a suspect has been collected, violating due process rights. [31] The use of this 'shared information' in judicial proceedings is only legislated for in two European countries. The UK[32] and the Netherlands[33] are currently the only European member states which have legislation that allows for the use of classified information in judicial proceedings. In the UK, they controversially have 'Closed Evidence Procedures' and the Netherlands allows a procedure known as 'shielded witnesses' which allows magistrates to examine intelligence officials in court.[34] The 2005 Piranha case in the Netherlands illustrates the use of the shielded witness act, where information provided by intelligence services formed a central component of the case and included a video message from one of the defendants. The defence team were unable to access the entire transcript of the video footage nor question intelligence officers.[35]According to Freedman, law enforcement and Intelligence communities were created and operate in line with a set of clear objectives which differ from one another. For example, law enforcement collects evidence in line with a set of concrete legal requirements, so that such evidence can be presented in court. On the other hand, intelligence agencies generally gather information in secret in the interests of national security, in a manner which is not designed for use in a court of law. [36] A report of the European Union's Agency for Fundamental Rights (FRA) pointed out that a separation between the police and intelligence services is important so as to avoid a 'concentration of power' within one service, in addition to protecting against the 'arbitrary use of information' gained by secret means.[37]

---

[31] Ibid.

[32] Justice and Security Act 2013 (JSA) codified previous legislation on closed court proceedings. See the full text of the Act at www.legislation.gov.uk/ukpga/2013/18/contents/enacted/data.htm.

[33] Act on Shielded Witnesses 2006 (*Wet afgeschermde getuigen*). Allows AIVD and MIVD to be heard before a special court. See full text of the Act at www.eerstekamer.nl/behandeling/20061024/publicatie_wet_14/document3/f=/w29743st.pdf

[34] Didier Bigo, Sergio Carrera, Nicholas Hernanz, Amandine Scherrer "National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges*, European Parliament*, Directorate-General of Policy Affairs" 2014, p.10

[35] Ibid., p.25

[36] Jonathan M Freedman "Intelligence Agencies, Law Enforcement and Prosecution Team" *Yale Law and Policy Review*, Vol. 16, No. 2, 1998, p.337

[37] European Union Agency for Fundamental Rights "FRA project on national intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies" Background paper for the inter-parliamentary conference on democratic oversight of intelligence services in the European Union, 2015, p.14

In 1999, the Parliamentary Assembly of the Council of Europe (PACA) stated that "[I]nternal security services should not be authorised to carry out law enforcement tasks such as criminal investigations, arrests, or detention. Due to the high risk of abuse of these powers, and to avoid duplication of traditional police activities, such powers should be exclusive to other law enforcement agencies".[38] In Germany, for example, the Act on the Federal Intelligence Service (BND) prohibits the attachment of the Intelligence Service to any police authority. In addition, countries such as Sweden ensure that the functions of the security services are kept separate from the police. However, even where services are kept separate, the FRA points out that the sharing of information is not necessarily prohibited. Bigo et al. found that a number of countries, including Germany, Spain and Sweden, allowed indirect judicial practices, which allowed certain evidence to be hidden from parties during trial. [39]In Spain for example, since 2000, second hand classified information can be used in judicial proceedings.[40] In this regard, they point to the European Commissioner of Human Rights statement that any information sharing should take place within a 'clear legal framework'. [41]

2. Non-Intelligence Actors and a Complex Web of Legislation

In most countries, the law bestows power upon Intelligence agencies and in turn defines the powers and mission of agencies. In addition, processes are defined and ascribed by law, providing an agency with clear guidelines and criteria with respect to 'working procedures'[42]. Special powers granted to intelligence services are usually restricted and outline: Who they are permitted to investigate, what information they are permitted to collect, what measures they can use when collecting information, and when they can use special powers and how long they are permitted to do so.[43] Legislation gives special powers to intelligence agencies, which are not generally available to other government and non-government actors, although in some circumstances these powers may be extended to some police services and

[38] PACE (1999), p. 2 in ibid
[39] Op. Cit., Didier Bigo et al., p.10
[40] Ibid.
[41] Ibid.
[42] Monica Den Boer, Claudia Hillebrand, Andreas Nolke "Legitimacy under Pressure: The European Web
of Counter-Terrorism Networks" *JCMS*, Vol. 46, no.1, 2008 p 107
[43] Aidan Wills "Guidebook: Understanding Intelligence Oversight, Geneva Centre for Democratic Control" *DCAF*, 2010, p.18

members of the public. [44] The range of actors currently exercising 'special powers' reserved for national intelligence agencies is a somewhat worrying development. In democratic societies, special powers should be the exception rather than the rule.[45] In addition, it raises serious questions about how effectively they can carry out intelligence functions in accordance with the law. In addition, where Intelligence agencies are involved in activities which are not related to their core functions, in particular as they relate to criminal prosecutions, it raises even more serious questions with regard to the protection of human rights.

A UK parliamentary report found that the current legal framework in the UK was overly complicated and difficult to understand and recommended that new legislation which would allow authorisations and safeguards to be applied consistently and transparently be introduced. They also recommended that existing legislation governing intelligence services be consolidated in to one law. [46] States should provide a clear and precise legal framework for all of the actors involved in the intelligence process. Given the absence of a single legal framework governing Intelligence activities[47], it is likely that questions will continue to abound with respect to the legitimacy of non-intelligence actors carrying out intelligence functions in the midst of a confusing web of legislation.

3. Intelligence Function and Structure: Legislating for the Intelligence System as a Whole

Steele argues that it is impossible for a single intelligence organisation to deal with current challenges associated with '24/7 coverage'.[48] Whilst it is necessary that intelligence agencies transform with respect to both their form and function in order to effectively combat the changing nature of threats, this transformation must be accompanied by appropriate legislation, which acknowledges this transformation and recognises the various actors involved in the process, not only in the interests of protecting human rights, but also to maintain effectiveness. The range of actors, both State and non-State, who are not part of the official intelligence structure, but carry out

---

[44] Ibid.
[45] Ibid.
[46] Intelligence and Security Committee of Parliament "Privacy and Security: A Modern Transparent Legal Framework" *House of Commons*. 2015, p. 103
[47] Op. Cit., Peter Roudick
[48] Robert David Steele "Information peacekeeping and the future of intelligence" 2003, in Op. Cit. Bob Hoogeboom, p.379

a range of functions which are central to the process, is clearly problematic, which raises the question whether the current trend towards integration in intelligence and 'across communities' has resulted in less effectiveness and more fragmentation. [49]

According to Walsh, establishing whether the intelligence sector is working effectively requires both a functional and structural approach.[50] Barger argues that in an ideal structure, the form an organisation should take should follow its function. It is therefore necessary when speaking about restructuring intelligence that this is preceded with a clear understanding of functions. These should be provided for clearly in the law. Barger also points out that the current size of the intelligence community requires treating intelligence in its entirety as a functional system and not 'merely as a blanket' covering a number of agencies and offices. She recommends a systemic view of the intelligence community, which would ensure that intelligence functions carried out by a range of actors are not coming in to conflict or replicating one another.[51] Taking a more holistic approach to intelligence, Canada has recently introduced legislation which will lead to the creation of a new oversight mechanism that will be responsible for overseeing the activities of all state actors involved in the Intelligence process, allowing a newly created National Security and Intelligence Committee of Parliamentarians to follow the entire process of intelligence carried out by any government department which has a national security function. Whilst this is a move in the right direction with respect to Intelligence oversight, it notably does not include oversight for non-state actors. [52]

Conclusion

With so many State and non-State actors now involved in intelligence activities, the legal framework governing Intelligence is becoming overly complex and fragmented, with a range of different laws regulating the behaviour of different actors in the intelligence process.

---

[49] Op. Cit., Patrick F Walsh, p. 123

[50] Patrick F Walsh "Building Better Intelligence Frameworks Through Effective Governance" *International Journal of Intelligence and Counter Intelligence*, Vol. 28, No.1, 2015, p. 125

[51] Ibid., p.43

[52] Craig Forsece, Kent Roach " A Report Card on the National Security Bill" *Institute of Public Policy Research*, 22 June 2017 @ http://policyoptions.irpp.org/magazines/june-2017/a-report-card-on-the-national-security-bill/

Within this complex web of legislation, it has become clear that some practices are not regulated appropriately, whilst others are not regulated at all. Adding to this, compliance is often weak, depending on what national oversight mechanisms, if any, a particular actor is subject to. Needless to say, the complexities and fragmentation, which exist within national legal frameworks, can be attributed to some extent to the reactionary and declaratory manner in which legislation is often enacted, with legislation been enacted without a thorough investigation into how such legislation will be implemented or if it will be effective. However, inherent problems with the system can also be attributed to the current disconnect which exists between intelligence as an organisational structure and intelligence as a process within the law. If legislators continue to ignore the intelligence system as a whole, both in terms of its structure and processes, laws are in danger of becoming ineffective or worse promoting ineffectiveness within the intelligence system.[53]

[53] Office of the Parliamentary Counsel "When Laws Become Too Complex"16 April 2013 @ https://www.gov.uk/government/publications/when-laws-become-too-complex/when-laws-become-too-complex

References:

1. Act on Shielded Witnesses 2006 (*Wet afgeschermde getuigen*). Allows AIVD and MIVD to be heard before a special court. See full text of the Act at www.eerstekamer.nl/behandeling/20061024/publicatie_wet_14/document3/f=/w29743st.pdf.

2. Akerboom, Erik, "Counter-terrorism in the Netherlands. General Intelligence and Security Service of the Netherlands" *AIVD,* 2000.

3. Bigo, Didier, Carrera, Sergio, Hernanz, Nicholas, Scherrer, Amandine, "National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges*, European Parliament*, Directorate-General of Policy Affairs" 2014.

4. Brown, Ian, Korff, Douw, 2009. Terrorism and the Proportionality of Internet Surveillance*, European Journal of Criminology*, Vol. 6, No. 2.

5. Den Boer, Monica, Hillebrand, Claudia, Nolke, Andreas, "Legitimacy under Pressure: The European Web of Counter-Terrorism Networks" *JCMS*, Vol. 46, no.1, 2008.

6. Chalk, Pater, Rosenau, William, "Confronting "the enemy within": security intelligence, the police, and counterterrorism in four democracies" *Rand*, 2004.

7. Chesterman, Simon, "We Can't Spy … If We Can't Buy! :The Privatization of Intelligence and the Limits of Outsourcing ' Inherently Government Functions, *The European Journal of International Law*, Vol. 19, No. 5, 2008.

8. Elshimi, M.S., *De-Radicalisation in the UK Prevent Strategy: Security, Identity and Religion* (Routledge, 2017).

9. Forsece, Craig, Roach, Kent, "A Report Card on the National Security Bill" *Institute of Public Policy Research*, 22 June 2017 @ http://policyoptions.irpp.org/magazines/june-2017/a-report-card-on-the-national-security-bill/

10. Freedman, Jonathan M., "Intelligence Agencies, Law Enforcement and Prosecution Team" *Yale Law and Policy Review*, Vol. 16, No. 2, 1998.

11. Gil, Peter, "The Implications of Intelligence Practice Within and Beyond the State: An Analytical Model*, Journal of Regional Security*" Vol. 8, No. 2, 2013.

12. Hoogenboom, Bob, "Grey Intelligence" *Springer*, Crime Law Soc Change, Vol. 45, 2006.

13. Innes, Martin, "Policing Uncertainty: Countering Terror through Community Intelligence and Democratic Policing" *AAPSS*, Vol. 605, May, 2006.

14. Innes, Martin, Sheptycki. James W. E.,"From Detection to Disruption: Some Consequences of Intelligence-led crime control in the UK'' *International Criminal Justice Review,* Vol. 14. 2004, pp.1-14.

15. Intelligence and Security Committee of Parliament "Privacy and Security: A Modern Transparent Legal Framework" *House of Commons*. 2015.

16. Krizan, Lisa, "Intelligence Essentials for Everyone" *Joint Military Intelligence College Washington D.C.*, Occasional Paper no. 6, 1999.

17. Lutterbeck, Derek, "Blurring the Dividing Line: The Convergence of Internal and External Security in Western Europe" *European Security*, Vol. 14 No. 2, 2005.

18. Martin, Siobhan, "Spying in a Transparent World: Ethics and Intelligence in the 21st Century" *GPSC*, Geneva Papers, Vol. 19, No. 16, 2016.

19. Office of the Parliamentary Counsel "When Laws Become Too Complex" 16 April 2013 @ https://www.gov.uk/government/publications/when-laws-become-too-complex/when-laws-become-too-complex

20. Roudick, Peter, "Foreign Intelligence Gathering Laws" *The Law Library of Congress*, 2006.

21. Steele, Robert David, "Information peacekeeping and the future of intelligence" 2003, in Op. Cit. Bob Hoogeboom.

22. UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/14/46.

23. Walsh, Patrick F., "Building Better Intelligence Frameworks through Effective Governance" *International Journal of Intelligence and Counter Intelligence*, Vol. 28, No.1, 2015.

24. Wills, Aidan, "Guidebook: Understanding Intelligence Oversight, Geneva Centre for Democratic Control" *DCAF*, 2010.

25. Zavrsnik, Ales, "Blurring the Line between Law Enforcement and Intelligence: Sharpening the Gaze of Surveillance?" *Journal of Contemporary European Research,* Vol. 9, No. 1, 2013.

INTELLIGENCE IN THE 21ST CENTURY

ANOTHER –*INT* ON THE HORIZON? CYBER-INTELLIGENCE IS THE NEW BLACK

Matteo E. BONFANTI *

Abstract

The pernicious nature of threats stemming from, or perpetrated through, the cyberspace is prompting the European and national decision-makers to adopt intelligence-led approaches for countering these threats. It pushes them to develop and employ targeted solutions to craft "cyber-intelligence" (cyber-INT) i.e. actionable knowledge of threat actors' intents and capabilities, as well as the vulnerabilities-opportunities they want to exploit. Similar to other cyber-related notions, there is no crystallised definition of "cyber-intelligence" (as a product and/or process) among both scholars and practitioners. Neither, it seems there are enough studies focusing on how it is crafted. In light of the above, the present paper tries to draw a clearer picture of this emerging practice by taking stock of the recently-promoted initiatives in the field and the existing analytical work on the topic. The paper starts by presenting the state of the art of cyber-intelligence programmes in the EU and in its Member States, and describes their recent developments. Then, it reviews the available scientific literature addressing cyber-intelligence. It discusses the notion of cyber-INT, examines how this intelligence is crafted through the lens of the (cyber) intelligence "cycle", and looks at the required capabilities (human, organisational and technological) for producing this kind of actionable knowledge. It concludes by sketching the main practical implications regarding the adoption of cyber-intelligence-led approaches, solutions and cooperation mechanisms across Europe.

Keywords*: Intelligence, Cyber-Intelligence, Cyber-Intelligence Process, Cyber-Security, Europe,*

Introduction

Since its foundation, the European Union (EU) and the Member States have supported the production and exchange of information and intelligence in order to enhance decision-making processes aimed at tackling targeted transnational security threats.[1] Aware that effective prevention of, and

* Senior Researcher Dr. *ETH Center for Security Studies, Zurich*, matteo.bonfanti@sipo.gess.ethz.ch

[1] Arthur Gruszczak, *Intelligence Security in the European Union. Building a Strategic Intelligence Community*, (London: Palgrave-McMillian, 2016).

response to, menaces posed by terrorism, organised crime, natural or man-made disasters need to be knowledge/intelligence-based, European and national policy-makers have progressively promoted relevant actions and collaborations in this field. They have established new agencies and tasked them with intelligence functions, improved the collection and analytical capabilities of existing bodies, as well as encouraged the (bilateral and multilateral) flow of information and insight among peer security/law-enforcement organisations.[2] Nowadays, the pervasive and pernicious nature of threats stemming from, or associated with, the cyberspace seems prompting European and national authorities to intensify their actions and mutual cooperation with regard to the gathering and sharing of relevant information and intelligence.[3] It seems pushing them – and other stakeholders as well – to develop and employ targeted organisational, procedural and technological solutions to sustain the crafting of actionable knowledge that can be consumed for engaging in effective prevention and response.[4]

Cyber-threats are actual or potential dangers to the networks and infrastructures the cyberspace consists of, or to the availability, integrity and confidentiality of the information contained therein. They are also menaces perpetrated through the cyberspace to targeted individuals, organizations and communities in the physical/real domain. They might stem out from different sources, involve a multitude of actors, be exercised by using several tools, and consist in a wide and evolving range of activities.[5] Cyber-threats may generate from conducts perpetrated by State and no-state actors to achieve a wide

---

[2] At the multilateral level, cooperation has generally proven to be fragmented and limited. This is due to different but interrelated "friction" factors. See Matteo E. Bonfanti, "Collecting and Sharing Intelligence on Foreign Fighters in the EU and its Member States: Existing Tools, Limitations and Opportunities", in A. de Guttry, C. Paulussen, F. Capone, *Foreign Fighters under International Law and Beyond*, (The Hague: Springer, 2016), pp. 333-353; Den Monica Den Boer, "Counter-Terrorism, Security and Intelligence in the EU: Governance Challenges for Collection, Exchange and Analysis" *Intelligence and National Security*, Vol. 30, 2015, pp. 402-419.

[3] There is no standard or universally accepted definition of "cyber-space" or "cyber-domain" (any spelling). The same goes for many other cyber-related terms *e.g.* "cyber-security", "cyber-threat", "cyber-attack", etc. Cf. https://ccdcoe.org/cyber-definitions.html. For the purpose of this essay, cyberspace is intended as a complex environment resulting from the interaction of several stakeholders, technologies, and practices. It is characterised by the processing of an ever-increasing wealth of information generated by the different activities that take routinely place in it.

[4] The reference to "actionability" is neither random nor trivial because it is what makes knowledge "intelligence".

[5] David Barnard-Wills & Debi Ashenden "Securing Virtual Space: Cyber War, Cyber Terror, and Risk", *Space and Culture*, Vol. 15, No. 2, 2012, pp. 110-123.

range of goals.[6] They may also originate from accidental events that compromise the correct functioning of, and accessibility to, information network infrastructures and systems. From a broader perspective, these conducts or events jeopardize the existence of those (State or non-state) organisations who rely increasingly, or are even critically dependent, on the information and services that are provided within or through the cyber-domain.[7] Having proper actionable insight into cyber-threats before/while they materialise can enable organisations to take preventive actions aimed at better safeguarding their interests and assets.

In Europe, a growing push towards the adoption of intelligence-led approaches/solutions for dealing with cyber threats comes from the members of the (not-formalised) European cybersecurity community. This community consists of representatives from supranational Institutions and agencies, domestic public bodies, private organisations, and the academia. Altogether, they contribute to shaping the discourse on cybersecurity in Europe and driving the actions that are taken within this policy area. The stakeholders of this community have already supported the definition and implementation of information/intelligence-led mechanisms for countering cyber-threats.[8] They have for instance sponsored the adoption of *ad-hoc* solutions for the delivery of "cyber-threat information/intelligence" (CTI), a product which should provide its consumers with the (technical) understanding of malicious networks operations and activities, and enable them to take subsequent actions.[9] However – at least as it is generally misconceived –, CTI alone does not prove to be fully suitable for enabling advanced prevention of cyber-

---

[6] *E.g.* State and State-sponsored actions may aim at gaining political, diplomatic, technological, commercial and strategic advantage; organised criminal groups generally aim at making illicit profit while terroristic networks o hacktivist have the goals of intimidating their victims or attract media attention.

[7] Nowadays, network and information systems and services – the Internet included – play a vital role in many contemporary societies. They have transformed, and are continuously shaping, the economic, social, institutional, and cultural life of several communities. Many of these systems are of public interest, and underlie the correct functioning of sensitive sectors of contemporary societies. This is, for example, the case of the automatic management and execution of processes that allow the functioning of critical infrastructures.

[8] Recently, EU Commission, "Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry", Brussels, 2016, OJ C 75, 10.3.2017, pp. 124-128, par. 2.2.2.

[9] Sharing of threat information, current attack patterns, software vulnerabilities and so forth has been standardised in process through the establishment of a network of CSIRTs (Computer Security Incident Response Teams) and been augmented by the establishment and development of a number of initiatives such as STIX/TAXII, CyBox, MISPs (Malware information Sharing Platform). See, e.g., http://stixproject.github.io/supporters/.

threats.[10] This is due to the technical nature and strictly operational scope of cyber-threat information/intelligence that allows its consumers to understand network events and trends ("inside the wire perspective"), and adopt reactive measures. Generally, CTI products are not build, and do not provide knowledge, on the wider and articulated context within which cyber-threats are framed.[11] They do not grant the understanding of cyber-threat ecosystems and do not enable advanced prediction/prevention.

By endorsing the idea that organisations should move from reactive to proactive security management postures and disapproving the attitude to interpret cybersecurity mostly as "measures taken after-the-event" and "static perimeter defence", some members of the European cybersecurity community are now sponsoring the adoption of concepts, tools and practices for the crafting and sharing of a more all-encompassing intelligence on cyber threats.[12] This intelligence should enable its consumers to comprehend the operational, tactical and strategic contexts of the threats (agents, capabilities, motivations, goals, impact, and consequences not only from a technical perspective), foresee their developments on the short-mid-long terms, and take informed decisions on the preventive actions to be taken. If integrated in their security-related decision-making processes, it should enable organisations to assume "predictive and anticipatory rather than past-oriented", "dynamic than static", and "agile and quick adaptable than rigid and conformed" postures toward cyber-related perils. The above described intelligence is often labelled "cyber-intelligence" (cyber-INT or CYBINT) – or intelligence "from", "for" and "within" the cyberspace – to differentiate it from the technically-interpreted and narrow-scoped "cyber-threat information/intelligence". In general, the expression cyber-intelligence is used to convey the idea of a wide-scoped and better qualified knowledge of actual or potential events occurring in the cyberspace that may endanger an organisation.[13]

Similar to many other cyber-related notions, there is actually neither a crystallised definition nor a real common understanding of "cyber-intelligence"

---

[10] Brian P. Kime, "Threat Intelligence: Planning and Direction", accessed 1 September 2017 at https://www.sans.org/reading-room/whitepapers/threats/threat-intelligence-planning-direction-36857. As stressed by the author, Indicators of Compromise (IOCs) like virus signatures and IP addresses, hashes of malware files or URLs or domain names of botnet command and control servers are not by themselves intelligence. They are information useful for network static defence. *Ibidem*, p. 3.

[11] Cf. Michael Montecillo, "Why Context is King for Enterprise IT Security", April 2014 accessed 1 September 2017 at https://securityintelligence.com/enterprise-it-security-context-king/.

[12] The term "proactive" should be here understood as the capacity to address actual of potential cyber-threats by strengthening defence and response measures.

[13] See also *infra*.

(as a product and/or process) among policy-makers, practitioner organisations, scholars, and the public opinion. If one looks at the relevant policies or mechanisms that have been recently implemented at the EU and Member States levels as well as other documentation issued by private and public organisations and the academia, "cyber-intelligence" is not always comprehensively defined or definitions vary. Despite the growing use of this or similar expressions not only by the media but also scholars and practitioners (especially by cybersecurity vendors for marketing reasons), current thinking on the subject is limited or not well-developed.[14] This holds especially true if one looks at the academic or other intellectual works on the topic that have been so far produced in Europe.[15] A deeper investigation of the subject – both from a theoretical and practical standpoint – is missing. On the contrary, the academic and practitioners' reflection on cyber-intelligence is relatively more advanced among the US security and cyber-security stakeholders.[16] This could be the consequence of the earlier adoption of cyber-intelligence related concepts, practices and technological solutions by US-based organisations.[17] However, given that the push toward the adoption of cyber-intelligence programmes seems to be on the rise also within European cyber-security

[14] Sometimes, the use of the expression or reference to the concept of cyber-intelligence looks like an expedient for making a certain product appealing to potential consumers. Well, the same can be said about the present paper and its author's goal.

[15] At least this seems to be the case of part of the literature reviewed for the purpose of writing this paper. *Cf.* Mario Caligiuri, *Cyber Intelligence. Tra libertà e sicurezza* (Roma: Donzelli, 2016), Id., "Cyber intelligence, la sfida dei data scientist", June 2016, accessed 1 September 2017 at https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/cyber-intelligence-la-sfida-dei-data-scientist.html, Antonio Teti, "Cyber Intelligence e Cyber Espionage. Come Cambiano i Servizi di Intelligence nell'era del Cyber Spazio" *Gnosis. Rivista Italiana d'Intelligence*, Vol. 3, 2013 pp. 95-121; Umberto Gori and Luigi S. Germani, *Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia* (Bologna: Franco Angeli 2012).

[16] Further to the literature that is cited *infra*, see also discussion that are held by US cybersecurity stakeholders on the Cyber Intelligence Blog available at https://cyberintelblog.wordpress.com/.

[17] See, *e.g.*, Office of the Director of National Intelligence, "The National Intelligence Strategy of the United States of America", 2014, pp. 1-24, accessed 1 September 2017 at https://www.dni.gov/files/2014_NIS_Publication.pdf. The strategy provides a definition of cyber-intelligence that reads as follow: "the collection, processing, analysis, and dissemination of information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, tactics, and operational activities and indicators; their impact or potential effects on national security, information systems, infrastructure, and data; and network characterization, or insight into the components, structures, use, and vulnerabilities of foreign information systems". *Ibidem*, p. 8. See also US Department of Defense Science Board, "Resilient military systems and the advanced cyber threat", January 2013, pp. 46 and 49, accessed 1 September 2017 at http://www.dtic.mil/docs/citations/ADA569975. Id., "The Department of Defence Cyber Strategy", April 2015, p. 24 accessed 1 September 2017 at https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

stakeholders, it would be worth deepening the discussion on this topic. In particular, it would be worth examining the notion of cyber-intelligence in more details as well as understanding the implications that may arise from the employment of cyber-INT-led approaches, methodologies, tools, and cooperation frameworks by the EU and national agencies and organisations.

The present paper intends to give a targeted contribution to the debate on cyber-intelligence. It tries to draw a clearer picture of this emerging practice by taking stock of the recently-promoted initiatives in the field and the existing analytical works on the topic. The paper starts by presenting the state of the art of cyber-intelligence programmes in the EU and in its Member States, and describes their recent developments. Then, it reviews the available scientific literature addressing cyber-intelligence. It discusses the notion of cyber-INT, examines how this intelligence is crafted through the lens of the (cyber) intelligence "cycle", and looks at the required capabilities (human, organisational and technological) for producing this kind of actionable knowledge. It concludes by sketching the main practical implications regarding the adoption of cyber-intelligence-led approaches, solutions and cooperation mechanisms across Europe. In general, the paper aims at two interrelated goals: improving the theoretical understanding of cyber-intelligence (academic-oriented goal), and outlining the broad issues regarding the promotion of cooperation on cyber-intelligence within the EU (practitioner-oriented goal).[18]

Cyber-intelligence and the Like across Europe

Often framed within the policy area of cybersecurity, different initiatives are presently promoted across Europe to sponsor the development and adoption of concepts, practices and technologies to timely identify, assess, prioritise and prevent existing or emerging cyber-related menaces.[19] Some of these initiatives make explicit use of the expression "cyber-intelligence" while others refer to the practice of generating actionable insight into cyber-threats through the collection, integration and analysis of both technical and broader contextual information about cyber-events. The notion of "contextual information" varies across the initiative at stake, its sponsors, their goals, as well as the type, object and scope of the crafted intelligence. In some cases,

[18] The paper arises from preliminary research activities that are currently carried out within a 3 years research project defined and run by author. Due to the limited number of pages here allowed and the early stage of the research project, the study will not go deep into all the salient issues that are identified.

[19] The EU cybersecurity architecture is described in EPSC Strategic Notes, "Building an Effective European Cyber Shield Taking EU Cooperation to the Next Level", Issue 24, 2017, p. 7, accessed 1 September 2017 at https://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf.

contexts are drawn by processing further technical data on malevolent conducts (type of tool employed, vulnerability exploited, etc.) that affect organisations; in others, they are defined through information on the geo-political, socio-economic, and cultural environments where cyber-threats generate from.

At the European Union level, Institutions and agencies foster the production and sharing of intelligence on cyber-threats for two main purposes: (i) to protect the European networks and information infrastructures from incidents or attacks; (ii) to enforce the law, *i.e.* prevent and counter the criminal use of cyberspace.[20] The first purpose concerns networks and infrastructures that are employed both within the civilian and military domain. As per the latter, the EU 2014 Cyber Defence Policy Framework calls for the protection of Common Security and Defence Policy (CSDP) communication networks by strengthening "cyber threat assessment and intelligence capability to identify new cyber risks and provide regular risk assessments based on the strategic threat assessment and near real-time incident information coordinated between relevant EU structures and made accessible at different classification levels".[21] On the practical side, the European Union Agency for Network and Information Security (ENISA) and Europol provide (among other things) information and knowledge to support the EU institutions, Member States' authorities, and other stakeholder communities to enhance their cyber-threats awareness and prevention/response capabilities and actions.[22] While

[20] This reflects the EU cybersecurity policy and architecture that are structured around three pillars: network and information security, law enforcement, and defence. *Cf.* EU Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN(2013) 1 final, Brussels, 7.2.2013, p. 10 and 17.

[21] Cf. Council of the EU, "EU Cyber Defence Policy Framework, Brussels", 18.11.2014, pp. 7, accessed 1 September 2017 at https://ccdcoe.org/sites/default/files/documents/EU-141118-EUCyberDefencePolicyFrame.pdf.

[22] ENISA is a centre of expertise in cybersecurity in Europe who assists the Union institutions, bodies, offices and agencies and the Member States in adopting and implementing the policies in network and information security, as well as enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security incidents. Further to Members States ENISA cooperate with the private sector. See Regulation (EU) 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, Strasbourg, in OJ L 165/41, 18.6.2013, pp. 41-58. Europol is the EU's agency whose main goal is to support and enhance Member States' competent authorities action and their mutual cooperation in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States. See Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council

ENISA's activities are mainly "IT-security management" oriented, Europol adopts law enforcement perspective and approaches to cybersecurity.

The former agency publishes – on yearly basis – the so called "ENISA Threat Landscape (ETL)" which offers an overview of identified cyber-threats, threat agents and current and emerging threat trends.[23] This (strategic) analytical product is mostly based on open source information even if some of the processed data are confidential. ETL aims to present the evolving cyber-threat environment and describe the top cyber threats and their components. It can be consumed by relevant organisations to define and plan new measures and security investments, as well as orient their existing cybersecurity strategies and actions. The content of ETL is referred to as "cyber-threat intelligence". Given the relevance of "contextual analysis" for the crafting of this product as well as its strategic scope, ETL should not be confused with the "narrow-scoped" threat information/intelligence (predominantly built upon IT-based data on artefacts/components). This is made evident by the methodology and models employed by ENISA to draft ETLs.[24] It is furthermore confirmed by the Agency itself when describing its position on CTI. As emerges from the 2016 ETL, the integration of contextual information and analysis is what the ENISA considers to be a necessary component to pass from "CTI information to knowledge".[25] However, within the ETLs crafting process, contextual information has specific meaning/scope. It covers the threat agents, their resources, modus operandi, used artefacts, threat positioning thorough the kill chain, related threats, evolving trends, and mitigation actions. In the ENISA's perspective these pieces of information and their interconnections make up the context of cyber-threats. As one may see, the

---

Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, Strasbourg, in OJ L 135, 24.5.2016, p. 53-114.

[23] Moreover, every year thematic threat landscapes are developed. These analytical reports present the cyber-threat exposure of particular sectors/application areas and propose mitigation strategies based on existing good practices. Further info at https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends. See for example, ENISA, Big Data Threat Landscape and Good Practice Guide, January 2016, accessed 1 September 2017 https://www.enisa.europa.eu/publications/bigdata-threat-landscape.

[24] Cf. ENISA, Threat Landscape Report 2015, Ch. 2.1; Threat Landscape Report 2014, Ch. 2.4.

[25] ENISA, Threat Landscape Report 2016 15 Top Cyber-Threats and Trends, January 2016, Ch. 2, accessed 1 September 2017 at https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016. This product is the fifth in a series of reports analysing cyber-threats.

technical connotation of information that is processed to draw the context is anyhow prevailing.[26]

With regard to Europol, its European Cybercrime Centre (EC3) delivers "cyber-intelligence" to fight cybercrime.[27] This intelligence results from the analysis of information on cybercrime that is gathered by the Centre from a wide array of public and private sources. It is delivered through the following products: (i) the "Cyber Bits", *i.e.* short intelligence notifications on cyber-related topics; (ii) the Open-Source Intelligence (OSINT) Dashboard, which reports the most important cyber-crime related events on weekly base; and (iii) the Common Taxonomy for the National Network of Computer Security Incident Response Teams (CSIRTs).[28] In EC3's perspective, each of these products represents cyber-INT. However, according to the available information, they look more like pieces of knowledge on cybercrime related issues than intelligence. At least this seems to be the case of the Common Taxonomy that is a nomenclature for the classification of cyber incidents or attacks. As per the OSINT Dashboard (therefore not cyber-INT!), it is open source information on the most important events in cybersecurity and cybercrime. With regard to "Cyber Bits", they consists of information on: (i) trends, *i.e.* emerging patterns and new *modi operandi*, tools and techniques that cyber criminals use; (ii) different related aspects of cybercrime such as infrastructure, tools and *modus operandi*; (iii) technical developments that could have an impact on the work of law enforcement authorities, and that can spawn more in-depth reports if it is felt that the initial findings warrant this; (iv) tools that have been developed at the request of a focal point within Europol, a Member State or a European Cybercrime Centre stakeholder.[29] Cyber Bits are generally offered to a large audience even if there are versions of this product that are delivered to law enforcement agencies only. Reasonably, the latter versions should contain more rapidly actionable knowledge, *i.e.* provide operational intelligence that enables short/mid-term actions. However, the actionability of the intelligence delivered through the Cyber Bits should not be over-estimated. As described by Europol, Cyber Bits bring important news to the attention of the law enforcement agencies rather

---

[26] This makes ENISA ETLs keen on being considered "tactical" cyber-intelligence. See *infra*.
[27] The EC3 was established in 2013 to strengthen the law enforcement response to cybercrime in the EU. Within the EC3 operates the Cyber Intelligence Team (CIT), whose analysts collect and process cybercrime-related information to identify emerging threats and patterns. More info at https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3#fndtn-tabs-0-bottom-1.
[28] *Ibidem*.
[29] *Ibidem*.

than providing them with a detailed assessment.[30] This put in to question their full qualification as intelligence. In general, despite the use of the expression cyber-intelligence by Europol EC3 to qualify its products, it is actually not completely clear what cyber-INT is and how it is crafted.

At the Member States level, the availability of intelligence on cyber-threats is acknowledged as a necessary requirement for engaging in effective prevention of and response to these threats. At least, this emerges from the latest policy instruments adopted and implemented by the British, Dutch, Spanish, Belgian, and Italian Governments to protect their national security and, in particular, improve cybersecurity. To a different extent and by using diverse wording, these instruments promote the mobilisation of relevant resources and capabilities for enhancing the production of intelligence, in particular, cyber-intelligence. This latter expression is formally employed by the Italian National Plan for Cyber-Security.[31] The Plan fosters the "strengthening of cyber-intelligence capabilities" and sustains the development of tools and processes for "the contextual analysis of cyber-events".[32] The definition of cyber-intelligence is provided by the updated version of the *Glossary on Intelligence* published by the Italian Information and Security System.[33] According to the Glossary, cyber-intelligence is the "Research and analysis of relevant information within or regarding the cyberspace in order to prevent, detect, contain and contrast threats to national security, for example, to critical infrastructures.[34] The expression "cyber-intelligence" is also employed by the Belgian Cyber Security Strategy for the defence sector.[35] It is defined as "Activities using all 'intelligence' sources in support of Cyber Security to map out the general cyber threat, to collect cyber intentions and possibilities of potential adversaries, to analyse and communicate, and to identify, locate, and allocate the source of cyber-

---

[30] *Ibidem*.
[31] "Piano Nazionale per la Protezione Cibernetica e Sicurezza Informatica", 2017, accessed 1 September 2017 at http://www.governo.it/sites/governo.it/files/piano-nazionale-cyber-2017.pdf.
[32] *Ibidem*, Indirizzo operativo 1, par 1.2.
[33] Sistema di Informazione per la Sicurezza della Repubblica, "Glossario Intelligence", December 2013, accessed 1 September 2017 at https://www.sicurezzanazionale.gov.it/sisr.nsf/quaderni-di-intelligence/glossario-intelligence.html.
[34] *Ibidem*. In Italian: "Ricerca ed elaborazione di notizie di interesse nel e sul cyber-space al fine di prevenire, rilevare, contenere e contrastare le minacce alla sicurezza nazionale, con riguardo ad esempio alle infrastrutture critiche".
[35] Belgian "Cyber Security Strategy for Defence" (English version), par. 8 accessed 1 September 2017 at https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf.

attacks.[36] No explicit mention of "cyber-intelligence" is given by the UK, Dutch and Spanish cyber-security strategies. With regard to the former, it encourages domestic intelligence and other security/law enforcement agencies to "expand their efforts to identify, anticipate and disrupt hostile cyber activities by foreign actors, cyber criminals and terrorists". According to the strategy "this will improve their intelligence collection and exploitation, with the aim of obtaining *pre-emptive intelligence on the intent and capabilities of our adversaries*" (emphasis added).[37] The Dutch strategy promotes the "Strengthening [*of*] research and analysis capabilities to gain more *insight into threats and risks in the digital domain*", while the Spanish expresses the Government's commitment to "enhance the national capabilities to detect and analyse cyber threats in order to generate the necessary *intelligence for a more effective defence and protection* of national networks (emphasis added).[38] Regardless of the used terminology, these latter reported passages insist on the production of actionable insight into threat actors' "intent and capabilities" or "threat and risks in the digital domain". Such insight should allow its consumers to adopt prevention (pre-empt and anticipate) and effective protection measures. Although not labelled as cyber-intelligence, it seems anyhow evident the reference to the acquisition of a more qualified knowledge than the one provided through narrow-scoped CTI.

Stronger than elsewhere is the push toward the employment of cyber-intelligence-led concepts and solutions that comes from the private sector. Several cyber-security vendors worldwide develop and offer tools and services to enhance their costumers' capabilities to identify and assess

---

[36] *Ibidem*, p. 18.

[37] The UK National Cyber Security Strategy 2016-2021, par. 4.16, 5.0.2, 6.2.5 accessed 1 September 2016 at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf. Cf. also "The National Security Strategy and Strategic Defence and Security Review 2015. A Secure and Prosperous United Kingdom", par. 4.107 and 4.114 accessed 1 September 2017 at https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015, stating that the Government will invest in capabilities to detect and analyse cyber threats, pre-empt attacks and track down those responsible. Furthermore, a new intelligence unit dedicated to tackling the criminal use of the "dark web" is established.

[38] The Dutch "National Cyber Security Strategy 2. From awareness to capability" (English version), Annex I, Objective 1, Action No. 1, accessed 1 September 2017 at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf. See also the Spanish "Estrategia de Ciberseguridad Nacional 2013", p. 31, accessed 1 September 2017 at http://www.lamoncloa.gob.es/documents/20131332estrategiaciberseguridadx.pdf.

potential cyber-threats to their assets.[39] Their proposed tools are often highly-technological. They combine artificial intelligence, machine learning, data analytics and other technologies to generate intelligence for cyber-threats prevention/response.[40] In general, vendors make clear that what they offer are not tradecrafts for the delivery of "technical feeds" on the menaces; they are instruments that produce intelligence through the collection, analysis and contextualisation of relevant threats.[41] Among other things, such an intelligence is premised upon the assessment of an organisation's activities and how they may prompt attacks, the understanding of the motivations and beliefs of a potential threat actor, the analysis of how a geopolitical event may trigger the use of a new attack type. In sum, it is based on the gathering and processing of not only technical data but broader contextual information.[42]

In light of what was described so far, it seems evident that different types of organisations across Europe endorse the idea of employing intelligence to prevent and counter cyber-threats. Sometimes called "cyber-intelligence" while other times not-labelled as such or not-comprehensively described, this knowledge should be crafted through the collection and analysis of information that is not confined to data on network operations and activities but covers broader aspects and implications of cyber-threats. Having said that, one may still wonder what cyber-intelligence more exactly is, and what its production implies. This would require a deeper investigation on the above described initiatives and examination of their adopted concepts and practices. It would also require to look at the intellectual/analytical work that has been carried out on the topic so far. The latter will the object of the following paragraphs.

Cyber-Intelligence: Looking for a Common Understanding

On Terminology and (shared) Definition

[39] The are several companies that provide these tools and services across the globe and Europe. Mapping them is beyond the scope of this paper. A collection of information about companies established in Europe will be included in the research project.

[40] See, *e.g.*, http://www.cyberintelligencecentre.com/.

[41] See *e.g.*: https://www.accenture.com/be-en/insight-accenture-cyber-intelligence-platform; https://www.microsoft.com/en-us/security/intelligence; https://dreamlab.net/en/services/cyber-intelligence/; http://www.silobreaker.com/; http://cscss.org/CIDC/, https://www.blackcube.com/cyber-intelligence/.

[42] Kristofer Månsson, "Why cyber should not be limited to cyber, in Business Reporter", May 2015, accessed 1 September at https://business-reporter.co.uk/2015/05/31/why-cyber-should-not-be-limited-to-cyber/. According to the author says "Cyber-events don't happen in a vacuum. There is context around them that often is hard to see".

In everyday language, "cyber-intelligence" (or whatever it is referred to) is mainly used as an enveloping and catch-all expression. A clearer picture of cyber-intelligence can be obtained by deconstructing the main conceptual elements that are involved in the initiatives that were described above, especially those that provide a definition of cyber-INT. However, this is not enough to understand what "cyber-intelligence" more exactly is. As a product and a process, is it intelligence "from", "on", "within" or "for" the cyberspace or some combination? To what extent does it focus on this space or cover events also occurring in the physical domain? What are the main sources of cyber-INT? How is it crafted? Is the "traditional" intelligence cycle applicable to cyber-intelligence? What are the implications in crafting and sharing cyber-intelligence? Answering to these framework – or other more specific – questions is not trivial.

For instance, the lack of a uniform understanding of the term "cyber" hinders any attempt to come up with a comprehensive and uniform notion of cyber-intelligence. Indeed, whereas it is more or less undisputed establishing what intelligence (as product and process) is, defining it in relation to the cyber domain is challenging.[43] In general, reflections on cyber-intelligence employ concepts, frameworks and terminology derived from the intelligence community and adopt/adapt them to the cyberspace.[44] This seems to be a logical approach given that some concepts are already established and there is no need to "re-invent the wheel". However, one may wonder to what extent these concepts are amenable to be applied to, and function for, a domain that differs from the traditionally known domains. The cyber is in fact a man-made, highly-evolving, technologically-shaped and not-fully tangible environment which, perhaps, needs to be interpreted by using different paradigms.[45] Its interaction with the physical domains are yet to be fully understood. Furthermore, cyber-intelligence is a relatively new practice which is far from being fully tested, assessed, and developed. There is not enough shared

[43] There are different definition of intelligence. Broadly speaking, intelligence is what is produced when collected information is analysed and evaluated. It is both a product and a process. It consists in the gathering, analysis, and the establishment of informed, targeted and actionable knowledge of the present, enabling accurate prediction of the future. It is worth stressing that such knowledge should be 'capable of being acted on or affording ground for an action'. Actionable knowledge is forward-looking. At its core, it is concerned with the possible future, with informed – indeed wise – estimates of future events.

[44] Robert M. Lee, "An Introduction to Cyber-intelligence", 2014, accessed 1 September 2017 at https://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/; Stephanie Helm, "Intelligence, Cyberspace and National Security", EMC Chair Conference paper, accessed 1 September 2017 at https://www.usnwc.edu/Academics/Faculty/Derek-Reveron/Workshops/Intelligence,-National-Security-and-War.aspx.

[45] This discussion, although very interesting, falls beyond the scope of this paper.

experience on how it works and on the best capabilities required to carry it out effectively. This hampers any attempt to come up with a thorough interpretative model for cyber-INT.

Having the above in mind is important for adopting a less biased and agnostic approach to cyber-intelligence and to the study of the topic. It helps in understanding why there is not yet an agreed and crystallised definition of cyber-intelligence. Actually, one may wonder whether it is really necessary or desirable to adopt a shared definition of cyber-INT. In principle, a definition can help relevant stakeholders to be consistent when they launch programmes or take actions on cyber-intelligence. It becomes a prerequisite when these stakeholders aim at establishing cooperation mechanisms in the field. This latter aspect is quite important. Indeed, the crafting process of cyber-intelligence requires (ideally) mutual collaboration and knowledge sharing.[46] To be effective and not fragmented, cooperation should be at least premised upon a common language and understanding of the conceptual components of cyber-intelligence and its crafting process.

Cyber-Intelligence: Actionable Knowledge "From", "Through", or "For" the Cyber?

According to the available sources, the study of cyber-intelligence dates back to 2010 when the US based Intelligence and National Security Alliance (INSA) established a Cyber Intelligence Task Force that published a first paper on the topic.[47] The paper set the framework to look at the cyber-domain through an intelligence-led perspective. It also presented the foundational thinking and approach to cyber-intelligence.[48] Since then, other analytical work has been carried out by the same organisation as well as other entities, experts and the academia.[49] The most part of this work pays attention to the notion of cyber-intelligence, the discussion on how this product is crafted, and functions at the strategic, tactical and operational levels within an organization. Military defence, national security, intelligence and cybersecurity are the fields of study within which relevant works are framed.

Basically, the literature describes cyber-intelligence as (the process consisting of and the product resulting from) the collection and analysis of

---

[46] See also *infra*.
[47] INSA is an organisation that facilitates dialogue and collaboration between the public, private, and academic sectors of the US intelligence and national security communities.
[48] INSA, Cyber Intelligence: Setting the landscape for an emerging discipline, 2011, pp. 1 – 20, accessed 1 September 2017 at https://www.insaonline.org/cyber-intelligence-setting-the-landscape-for-an-emerging-discipline/.
[49] See *infra* the footnotes.

information to support decision making on cyber-threats. Depending on the scope of the information gathering activities, the means employed to carry them out, and the final purpose they serve, there are actually two ways to look at/interpret cyber-intelligence.[50]

One way is to think about cyber-INT as intelligence "from" the cyber, *i.e.* knowledge produced through the analysis of any valuable information collected "within" or "through" the cyberspace. This is cyber-intelligence "stricto sensu". From this perspective, "cyber-" refers to both the domain where data are sourced or, in other, words, that vast digital repository of information amenable to be retrieved and processed; and the tools/ techniques/media through which these data are collected (*e.g.* via Computer Network Exploitation technologies and techniques).[51] According to this interpretation, cyber-INT can in principle support decision making in any domain and not only to counter cyber-threats. It can support a broad variety of missions in government, industry, the academia including policy-making, strategic planning, international negotiations, risk management, strategic communication in further areas than cyber-security. In other words, cyber-intelligence may operate "independently and does not necessarily need to support a cybersecurity mission".[52] However, given that cyber-intelligence is often discussed in relation to cybersecurity or to the prevention of and response to cyber-threats, these are the primary – but, again, not exclusive – goals of this kind of intelligence.

Another way to interpret cyber-INT is considering it as intelligence "for" the cyber, *i.e.* insight that stems out from an all-source intelligence activity occurring within and outside the cyberspace. It is cyber-intelligence "lato sensu". In this sense, the intelligence "for" the cyber can also include (or be built on) intelligence "from" the cyber. It can draw from any intelligence discipline that supplies crucial knowledge, regardless of the source, method, or medium employed for crafting it. As such, cyber-intelligence may therefore result from the combination of Open Source Intelligence (OSINT), Signal Intelligence (SIGINT), Geospatial Intelligence (GEOINT), Social Media

---

[50] Matthew M. Hurley, "For and from Cyberspace Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance" *Air & Space Power Journal*, Vol 26, No. 6 (2012), pp. 12-33.

[51] Ross W. Bellaby "Justifying Cyber-intelligence?", *Journal of Military Ethics*, Vol. 15, No. 4, (2016), pp. 299-319; Matthew M. Hurley, cit., p. 13. Computer Network Exploitation or cyber exploitation refers to the secret collection and reproduction of digital data from computers or networks.

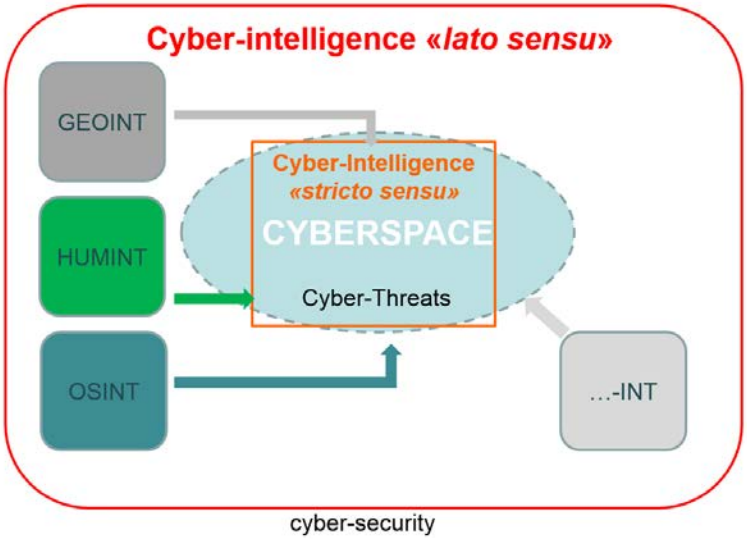
[52] Troy Townsend, Melissa K. Ludwick, Jay McAllister, Andrew O. Mellinger, Kate A. Sereno, "Cyber Intelligence Tradecraft Project: Summary of Key Findings", the Software Engineering Institute (SEI) Emerging Technology Center at Carnegie Mellon University, September 2013, pp. 2.01-2.20, spec. 2.5 at http://www.sei.cmu.edu/about/organization/etc/citp-summary.cfm. The full report is available at http://www.sei.cmu.edu/about/organization/etc/citp.cfm.

Intelligence (SOCMINT), and Human Intelligence (HUMINT).[53] From this point of view, cyber-intelligence is less a discipline itself than an analytic practice relying on information/intelligence collected also through other disciplines and that is intended to inform decision makers on issues pertaining to activities in the cyber domain.[54] What qualifies this kind of intelligence as "cyber-" is the purpose for which it is crafted: support decision making on cyberspace related issues.

The two discussed perspectives on cyber-intelligence – intelligence "from" and "for" the cyber – are often condensed in to one single comprehensive concept (Figure 1). This is also due to the fact that intelligence "for" the cyber actually incorporates the one "from" the cyber. The result is a broader notion of cyber intelligence that includes the collection, processing, evaluation, analysis, integration, and interpretation of information that is available "within", "though" and/or "outside" the cyberspace to enhance decision-making on cyber-related menaces. The described notion of cyber intelligence seems to correspond to the one endorsed by the Belgian Strategy for Cyber-Security for the Defence and the Italian Cyber Security Strategy (*cf.* the Glossary).[55]

Figure 1. Cyber-intelligence "stricto sensu" and "lato sensu"

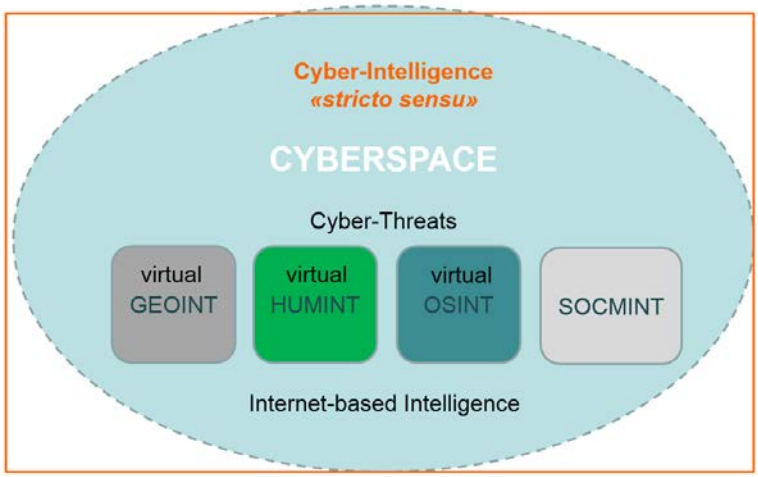
[53] Aaron F. Brantly, *The Decision to attack. Military and Intelligence Cyber-Decision Making*, (Athens GA: The University of Georgia Press, 2016), Ch. 7, pp. 103-108 and 116-121.
[54] INSA, Operational Levels of Cyber Intelligence, September 2013, pp. 1-14, accessed 1 September 2017 at https://www.insaonline.org/operational-levels-of-cyber-intelligence/. On the existing intelligence disciplines, see among others The UK MoD, "Joint doctrine publication 2-00, understanding and intelligence support to joint operations", JDP 2-00, 2011, accessed 1 September 2017 at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf. In Italian: Glossario intelligence, cit.
[55] See *supra*.



However, it is worth noting that when looking at the "traditional"-INT disciplines encompassed by the notion of cyber-intelligence "lato sensu", their narrower and circumscribed projection to the cyberspace has determined the development of *ad hoc* concepts and approaches (or simply reference to expressions) like: virtual HUMINT, virtual or internet-based OSINT, virtual COMINT, etc (Figure 2). The adjective "virtual" indicates that intelligence activities are carried out within the cyberspace or through computer-generated tools (intelligence "stricto sensu"). Its association with "traditional" –INT concepts/ practices is made for referring to the adoption of methods/approaches/tools that are employed by these practices and adapted for the cyberspace.[56] A bit different from the above concepts is the notion of social media intelligence (SOCMINT) which is considered by some scholars/practitioners as having proper features that can be difficulty linked to other intelligence disciplines.[57]

Figure 2. Virtual -INTs

[56] For example, the virtual HUMINT approach aims at collecting tactical/operational intelligence from the information generated by members of virtual communities. Practically, it consists in establishing and operating a virtual identity (avatar) to gain trust from, and create long-term relationships with, the members of the participated/monitored communities, as well as recruit, handle, manipulate and decept them with the purpose of collecting information. As evident, it adopts and relies on HUMINT traditional approaches but apply and adapt them to the cyberspace. One may wonder to what extent it is possible to consider virtual HUMINT a specific sub-category of HUMINT or think about it as an emerging practice. Answering to this question would require examining in more details the differences and similarities between these activities and the functions they consist of. However, this is far beyond the scope of the present paper.
[57] Omand et al., "#Intelligence". Cf. Bonfanti, "Social media intelligence", 231-262.



With regard to the information to be retrieved, this may range from network technical data (*e.g.* hardware and software data), data on hostile organizations and their capabilities, ongoing cyber activities, to potentially any relevant geopolitical event.[58] The type of data as well as their classification are not functional to the definition of cyber-intelligence. Data can be raw or already processed information; they can be obtained – legally or through unlawful intrusion/exploitation actions – from open, proprietary, or other classified sources.[59] Actually, as the literature suggests, multiple sources of information are needed to develop a more holistic understanding of the threat environment and producing comprehensive cyber-INT.[60] The most important aspect of the data is that they should be (somehow) validated.[61] When analysed, information should allow decision makers to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action.[62] This is the main feature of cyber-intelligence, *i.e.* its enabling goal: to provide its consumers with insight into potentially hostile activities that may

[58] Jung-ho Eom, "Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace" *International Journal of Software Engineering and Its Applications* Vol. 8, No. 9, 2014, pp.137-146. The article deals with cyber- intelligence for military purposes.
[59] Robert M. Lee, "Cyber Intelligence Collection Operations", 2014, accessed 1 September 2017 at https://www.tripwire.com/state-of-security/security-data-protection/cyber-intelligence-collection-operations/.
[60] INSA, cit., p. 1.
[61] Validation is often a challenging task due to the high volatility, anonymity and uncertainty of data and heterogeneity of data sources.
[62] Troy Townsend, Melissa K. Ludwick, cit.

occur in the cyber domain or be perpetrated through the cyberspace, and allow them to design effective preventative (proactive) or counteractive (reactive) measures.

Depending on its scope or level of actionability, cyber-intelligence can be strategic, tactical or operational.[63] There is actually no uniform interpretation of what the different levels of cyber-INT should consist in. According to the large part of the available literature, strategic cyber-INT focuses on the long-term, typically reviews trends in current and emerging threats, as well as examines opportunities to contain these threats. It serves apical decision making processes aimed at the achievement of an organization's mission, the determination of its direction and objectives. It covers the threat landscape for macro trends (*e.g.* political, social, economic) affecting the organization and identifies who are the threat actors, what are their goals, why, and how they will likely attempt to achieve them. It is rich in contextual information.[64] Tactical cyber-intelligence concerns what is happening on the network. It also examines the strength and vulnerabilities of an organisation, and the tactics, techniques and procedures (TTPs) employed by threat actors.[65] Due to its nature and reach, tactical cyber-INT corresponds to what is generally meant as cyber-threat intelligence.[66] Generally more technical in nature, it informs the specific network-centred steps and actions the organization takes to protect assets, maintain continuity, and restore operations. As far as operational cyber-INT is concerned, it consists into knowledge on imminent or direct threats to an organisation. It enables and sustain day-to-day operations and output. At this level, cyber-intelligence looks at the organization's internal processes and vulnerabilities.[67]

---

[63] The INSA defines each operational level of cyber intelligence according to: (i) the nature, role and identity of the consumer; (ii) the decisions the consumer will make; (iii) the timeframe in which the consumer tends to operate; (iv) the scope of collection; (v) the characterization of potential adversaries; and (vi) the level of technical aptitude required for cyber intelligence collection. See references in the next footnotes. *Cf.* also Randy Borum, "Getting Left of the hack. Honing Your Cyber Intelligence Can Thwart Intruders", September 2014, accessed 1 September 2017 at https://works.bepress.com/randy_borum/63/; INSA, cit., pp. 7 ff.

[64] Randy Borum, John Felker, Sean Kern, Kristen Dennesen, Tonya Feyes, "Strategic Cyber Intelligence" *Information & Computer Security*, Vol. 23, No. 3, 2015, pp. 317-332. See also, INSA, Strategic Cyber intelligence, 2014, pp. 1-16 accessed 1 September 2017 at https://www.insaonline.org/strategic-cyber-intelligence/.

[65] INSA, Tactical Cyber Intelligence, 2015, pp. 1-16 accessed 1 September 2017 at https://www.insaonline.org/tactical-cyber-intelligence/.

[66] See *supra*.

[67] INSA, Operational Cyber Intelligence, 2015, pp. 1-16 accessed 1 September 2017 at https://www.insaonline.org/operational-cyber-intelligence/.

It worth repeating that the described distinction between the levels of cyber-INT is mainly scholastic. In practice, there is no clear demarcation from one level of intelligence to another; they frequently overlap or are combined. Furthermore, the meaning of strategic, tactical, and operational is likely to vary across organizations because of their size, complexity, mission and related attributes.[68] Regardless of any clear-cut demarcation among the levels, quite important is the capacity of an organisation to consider all these levels and craft intelligence that allows it to understand the challenges and opportunities it is likely to encounter in the short-mid-long terms. As a finished product, it seems there are no established formats or standards for presenting cyber-intelligence to decision-makers.

What has been discussed so far helps in drawing a clearer picture of cyber-intelligence and identifying the main conceptual components involved in its notion – at least the one identified by the literature? Further comprehension of cyber-INT can be obtained through the discussion of how this product is crafted. Such a discussion requires the examination of those set of (sequential?) operations resulting in cyber-INT and the required capabilities (human, organisational and technological) to carry them out.

The Cyber-Intelligence Process: Alternative *vs* Traditional Models

Just like the case of other intelligence products/disciplines, cyber-intelligence is crafted through a set of activities/functions (that has collection and analysis at its core). Traditionally, this set of functions is represented and explained through the "intelligence cycle" model.[69] The model has been studied and questioned several times by practitioners and academics to the point that alternative models were proposed and discussed.[70] The "validity/applicability" of the traditional intelligence cycle model is also questioned as far as cyber-intelligence is concerned. As it is argued, the traditional model has a limited applicability to the cyber and cannot accurately explain the crafting process of cyber-intelligence. Meant as a linear and reiterative cycle, it does not emphasize the inter-related nature of the

---

[68] INSA, Strategic Cyber intelligence, cit. p. 4.

[69] While there are different representations of the Intelligence cycle, the most common comprises five distinct phases: Planning and Direction, Collection; Processing, Analysis, and Dissemination. The logic of the intelligence cycle lies in the assumption that consumers of the finished intelligence make decisions on the basis of this product, and these decisions may lead to the levying of more requirements, thus triggering the cycle again. On the intelligence cycle see Mark Phythian (Ed.), *Understanding the Intelligence Cycle* (London and New York: Routledge 2013).

[70] *Ibidem*.

activities (planning, collection, processing etc.) the cyber-intelligence process consists of, and their mutual relevance. In other words, it does not capture their inter-dependencies and mutual influences.

In light of the above, an alternative model is proposed to explain the cyber-intelligence process.[71] It differs from the traditional intelligence cycle for the adopted terminology, the non-linear and strictly consequential logic of the functions the process consists of, the decomposition of the analysis function in to two specialised functions (the technical or functional analysis and the strategic analysis), and the capacity to capture both the "narrow" technical cybersecurity and "wider" cyber-threats prevention purposes that cyber-intelligence can serve within an organisation. As it is represented, the proposed model accommodates the interpretation of cyber-intelligence as an analytic practice relying on information/intelligence collected also through other disciplines and which is intended to inform decision-makers on issues pertaining to activities in the cyber domain.[72]

The proposed model consists of five functions: (i) the determination of the "Environment" which establishes the scope of the cyber intelligence effort and influences what information is needed to accomplish it;[73] (ii) the "Data Gathering" *i.e.* the exploration of data sources and collection-filtering of information through automated and labour-intensive tools;[74] (iii) the "Functional Analysis", *i.e.* the performance of technical and tailored analysis (typically in support of a cybersecurity mission) that is aimed at deriving the

---

[71] Troy Townsend, Melissa K. Ludwick, *et alii*, cit.

[72] *See supra*.

[73] Troy Townsend, Melissa K. Ludwick, *et alii,* p. 2.9. Environment is meant as both internal and external. The determination of the internal environment includes the studying of an organisation's global cyber presence, the infrastructure that are accessible through the Internet, as well as the definition of what data needs to be collected to maintain network situational awareness. Externally, the determination of the environment requires to know which the entities capable of affecting organizations' networks are. It requires to find out and map system vulnerabilities, intrusion or network attack vectors, and the tactics, techniques, procedures, and tools used by relevant threat actors. As it is suggested: "By investing the time and energy to define the environment, organizations significantly improved their data gathering efforts, resulting in more efficient and effective cyber intelligence programs".

[74] *Ibidem*, p. 2.11. Data gathering should cover both internal (*e.g.,* net-flow, logs, user demographics) and external sources (*e.g.,* third-party intelligence providers, open source news, social media). It should focus on the pertinent threats and strategic needs as identified while learning about their organization's environment. Indeed, to be effective data gathering should be based on the definition of the environment. It should target the necessary data for conducting meaningful analysis on critical cyber threats.

"what" and "how" of cyber threats;[75] (iv) the "Strategic Analysis" entailing the review, integration with contextual information, and further elaboration of the functional cyber-intelligence with the goal of answering the "who" and "why" questions;[76] and (v) the decision maker "Reporting and Feedback", *i.e* dissemination of cyber-intelligence to decision makers and collection of feedback.[77]

The main dependencies and mutual influences among the described functions are the following. Data gathering should be premised upon the determination of the environment which is itself influenced by the decisions taken by the organisation on the basis of consumed cyber-intelligence. The intelligence resulting from the functional analysis can inform decisions on actions to be taken on the technical-network level of an organisation which, in turn, impact on the determination of the internal environment; the same goes with intelligence resulting from the strategic function which impact on both the internal and external environment. The strategic function also renders the intelligence resulting from the functional analysis more consumable by apical decision makers who may not have a technical background. From this perspective, it is a sort of add-on application who contributes in bridging the communication gap between analysts and top decision makers. These latter provide their feedback on the received intelligence to shape analytical functions, adjust the direction of the organisation and therefore influence the environment.

Questioning the "validity" of the discussed cyber-intelligence process model is beyond the scope of this paper. However, there are few considerations that are worthy of being made. First of all, the proposed model has been designed following an empirical work which mapped and assessed current practices in cyber-intelligence in the US. It is grounded on data and represents what the state of the art within selected organisations. It has also a normative reach *i.e.* suggests how the process should work to be effective. Furthermore, the proposed model has the advantage to be relatively simple while, at the same time, representative of practices adopted by different types of organisations *e.g.* small corporations, larger industries, and governmental

---

[75] This function includes the verification/validation of data based on the quality of the source, reporting history and independent verification of corroborating sources. *Ibidem*, p. 2.13.
[76] *Ibidem*, 2.15. Strategic analysis adds perspective, context, and depth to functional analysis. It is ultimately rooted in technical data, but incorporated information outside traditional technical feeds. The resulting strategic analysis populated threat actor profiles, provided global situational awareness, and informed decision makers of the strategic implications cyber threats posed to organizations, industries, economies, and countries.
[77] *Ibidem*, p. 2.17.

agencies. However, its representativeness is likely to fade away at both the lower and higher levels of occurrence of the cyber-intelligence process *i.e.* at the individual and multi-partnership or transnational levels. Especially at the latter level, the degree of organisational/institutional complexity will probably render the intelligence model unfitted. In addition, technological developments that are likely to occur in the field of cyber will probably impact on the model and require further re-elaborations.[78] Lastly, the proposed model still suggests that collection and analysis are sequential *i.e.* the latter can only begin once the former is complete. In practice, the two functions are interactive and occur concurrently. The above said, the described model represents a sound attempt to better explain how cyber-intelligence is (should be) crafted.[79]

The Most Wanted: Skilled Analysts and Advanced Analytics

As one may understand, producing valuable cyber-intelligence requires an organisation to acquire significant capabilities in terms of human, technical, organisational, and financial resources. It also requires the adoption of tailored and effective procedures.[80]

As far as the human resources are concerned, the cyber-intelligence crafting process should rely on skilled individuals to perform the collection and the analysis of information as well as the communication of the resulting intelligence to decision-makers. On top of the characteristics (traits and competences) any intelligence practitioner should possess (*e.g*. understanding the intelligence requirements, defining a problem, apply research and analysis methods and think strategically to suggest a course of action), the cyber-intelligence operator should combine a mix of technological and human and social science culture/skills.[81] This is required by the nature of cyber-intelligence that demands analysts to deal with technical data on information systems, networks and tools, as well as broad contextual information of

[78] This is actually acknowledged by the promoters of this model when discussing about analytical capabilities. "Because technology changes so quickly, the process of producing cyber intelligence analysis had to be dynamic enough to capture rapidly evolving tools, capabilities, and sophistication of adversaries".

[79] A deeper discussion of the cyber-intelligence process as well as the formulation on another alternative interpretative model will be carried out within the research project.

[80] Needless to say this hold also true with regard to other intelligence practices.

[81] Melissa K. Ludwick, Troy Townsend, Joan P. Downing, "White Paper – CITP Training and Education", Sep 2013, 6.1-6.24, accessed 1 September 2017 at http://www.sei.cmu.edu/about/organization/etc/upload/whitepaper.pdf.

different typology. The operator's knowledge should in principle span from operating systems and scripting and coding techniques, to geopolitics, terrorism, and organised crime. Since it is most unlikely that one person possesses such a broad and overarching knowledge, what cyber-INT operators should principally have is the aptitude to be collaborative and keen on working in multidisciplinary teams – within which sectorial competencies can be combined.

To a significant extent, collection and analysis can be automatized through the employment of advanced technologies.[82] These can assist cyber-intelligence practitioners to search and retrieve data and make sense of them. Regardless of any specific feature of the employed technological solutions, it worth stressing that these are to be meant as tools that assist practitioners with performing cyber-INT and speed-up data processing and analysis. They do not carry out all the cyber-INT process' functions and deliver ready-to-be-consumed intelligence. Furthermore, given the nature of cyber-INT, analytics should be able to perform processing, correlation, integration, visualisation of large sets of data that have different format and stem from diverse sources which are explored through various intelligence disciplines.[83] Even if capable to do that in an effective manner, the process will anyhow benefit from the practitioner' personal traits, competencies and experience. In conclusion, although amenable to be executed with the extensive support of technological tools, cyber-intelligence as a process requires – and cannot get rid of – human operators (and their human brain!).

Crafting and Sharing: Two Faces of the Same Coin

Another aspect concerning the crafting of comprehensive cyber-intelligence is the need to have access to multiple sources of information or knowledge. This is often not possible for a single organisation who therefore needs to be provided with data, or even finished intelligence, by external entities. Regardless of the basis (voluntary or mandatory) upon which the provision of data and knowledge takes place, this should in principle occur regularly and be framed within a (formal or informal) cooperation mechanism which has information sharing as object.[84] Indeed, the crafting of cyber-intelligence can significantly benefit from the integration and analysis of

---

[82] *Cf.* also *supra*.
[83] *Cf.* also *supra.*
[84] AFCEA International Cyber Committee, "Cyber Intelligence Sharing", 2014, accessed 1 September 2017 at https://www.afcea.org/committees/cyber/documents/AFCEACyberIntelligenceSharingPaper-FinalVersionforPublication_002.pdf.

information or further intelligence that are dispersed across sources accessible by third parties only (*e.g.* governmental agencies, private organisations, academia) and then shared.

Same as for other -INT disciplines, the production and the sharing of cyber-intelligence are interrelated processes.[85] They are actually more interrelated than it would seem at the first sight. Indeed, cooperation among cyber-intelligence stakeholders – at both the domestic and international level – may contribute to crafting more valuable intelligence, *e.g.* making accurate, complete and corroborated threat assessments and predictions. Having multiple actors – each of them with specific remit and capabilities in information and intelligence gathering – that combine the knowledge they have respectively acquired may result in "enhanced" cyber-intelligence products to be consumed for designing more effective preventive and counter-measures. Put differently, the enhanced cyber-intelligence products that may result from improved information sharing could provide more sound intelligence support to face cyber-threats; and the more this support proves to be sound and actionable, the more – in principle – relevant stakeholders are likely to incentivise the sharing of cyber-intelligence.

The above argument seems to work well in principle. The reality sounds different: organisations tend to limit their engagement in information or intelligence sharing. Differently from the case of "general" intelligence cooperation, the production and sharing of cyber-intelligence face further hurdles. These latter have been already documented with regard to the exchange of "information" – not intelligence – in the context of network and information security.[86] The same goes with the limits to the sharing of "cyber-threat intelligence".[87] Some of the identified hurdles are attributed to significant involvement of private actors in the production and sharing of cyber-intelligence. These actors play a central role in the collection of information that is relevant for determining the threats landscape. In general, they are not keen on sharing this information, or exchanging their in-house produced intelligence, for different reasons (reputational risks, protection of sources, unwanted transfer of technological knowledge, and legal liability) among which the general lack of trust of their peers or other involved

---

[85] Matteo E. Bonfanti, cit.

[86] *Cf. e.g.* ENISA & RAND Europe, "Incentives and Challenges to Information Sharing", 2010, accessed 1 September 2017 at https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing.

[87] *Cf. e.g.* CERT-UK, "Integrating Threat Intelligence. Defining an Intelligence Driven Cyber Security Strategy", 2015, at https://www.cert.gov.uk/wp-content/uploads/2015/03/CPNI CONTEXT_CERT-Threat_Intelligence.pdf.

stakeholders – both national and international. In conclusion, poor cyber-intelligence cooperation may result in degraded overall prevention of, and response to, cyber-threats.

Conclusions: Which Way Forward to Establishing Cyber-Intelligence Mechanisms in Europe?

As above discussed, there is a growing push towards the adoption of intelligence-led concepts, approaches and solutions to counter cyber-threats in Europe. This push comes from different representatives of the European cyber-security community. Initiatives in the field have already been promoted by the EU, its Member States and other private organisations. Some of these initiatives address the crafting of "cyber-intelligence" specifically. Although not always defined, cyber-INT is generally meant as the practice that consists in the gathering and analysis of an all-source of information/intelligence to prevent and contrast cyber-threats. Basically, this interpretation corresponds to the notion of cyber-intelligence discussed by the available literature on the topic. The same literature which also explains how cyber-INT is (should be) crafted and identifies the required capabilities for producing it.

Regardless of any manifested intention to go for the adoption of cyber-intelligence concepts or solutions by European or national agencies and organisations, the effective implementation of dedicated programmes in the field requires significant efforts by their promoters. It requires a better understanding of what cyber-INT is and the purposes it can serve, the acknowledgment of the challenges surrounding its crafting process, the identification of the actors that should be involved in the process, and the determination of the resources that are needed to acquire the relevant capabilities. As per the latter, it seems paramount for organisations to invest in the employment of skilled cyber-INT operators or support the run of *ad-hoc* training for internal resources. It is likewise important for them to sustain the development and acquisition of technological tools to be employed for the collection and analysis of information stemming from multiple sources. All this should be combined with the adoption of tailored organisational structures and internal processes. Furthermore, given the above discussed interrelation between the production and the sharing of cyber-intelligence, *ad hoc* cooperation mechanisms to foster the flow of information or finished cyber-intelligence among relevant actors should be established. Cooperation may occur bilaterally or multilaterally. If possible, it should involve the transnational level too. As per the latter, it does not seems that the EU can support the flow of information and intelligence on cyber-threats more than it

presently does within the ENISA and Europol. Given its close ties to Member States' national (cyber-) security (falling within their national sovereignty and domestic jurisdiction), the sharing of cyber-intelligence would require enhanced cooperation among the EU Member States – which is not in place at the moment. However, the EU institutions and their agencies can provide structured platforms for discussion and further negotiations. At the domestic level, cooperation mechanisms should be established within private and public cybersecurity stakeholders. As already pointed out, there are still several obstacles in establishing such cooperation frameworks. However, the growing reach of the menaces coming from the cyberspace and the (yet to be fully) spread awareness of the "need to share" among cyber-intelligence stakeholders would probably induce them to improve their initiative in information/intelligence sharing.

There is a final annotation. The use of the word "practice" rather than "discipline" across this paper is not random. Although the most part of the literature considers cyber-INT being an already-established or soon-to-become-established discipline, it does not seem the case – at least in Europe. The lack of a more mature theoretical elaboration of cyber-INT coupled with the relatively limited experience on it, makes it difficult to consider this type of intelligence a recognised area or branch of intelligence. In other words, cyber-INT should not be considered a discipline because it has not yet been sufficiently defined and practiced. Furthermore, as described above, the nature of cyber-INT and its crafting process makes it less a discipline than an analytic practice which relies on information/intelligence collected also through other disciplines. Of course, nothing prevents cyber-INT to establish itself as a discipline which employs specific technical or human resources throughout the different functions of its crafting process.

References:

1. AFCEA International Cyber Committee, "Cyber Intelligence Sharing", 2014, accessed 1 September 2017 at https://www.afcea.org/committees/cyber/documents/AFCEACyberIntelligenceSharingPaper-FinalVersionforPublication_002.pdf.

2. Barnard-Wills, David, Ashenden, Debi, (2012), "Securing Virtual Space: Cyber War, Cyber Terror, and Risk", *Space and Culture*, Vol. 15, No. 2, 2012, pp. 110-123.

3. Bellaby, Ross W. "Justifying Cyber-intelligence?", *Journal of Military Ethics*, Vol. 15, No. 4, (2016), pp. 299-319; Matthew M. Hurley, cit., p. 13.

4. Bonfanti, Matteo E., (2016), "Collecting and Sharing Intelligence on Foreign Fighters in the EU and its Member States: Existing Tools, Limitations and

Opportunities", in A. de Guttry, C. Paulussen, F. Capone, *Foreign Fighters under International Law and Beyond*, (The Hague: Springer, 2016), pp. 333-353;

5. Borum, Randy, "Getting Left of the hack. Honing Your Cyber Intelligence Can Thwart Intruders", September 2014, accessed 1 September 2017 at https://works.bepress.com/randy_borum/63/; INSA, cit., pp. 7 ff.

6. Borum, Randy, Felker, John, Kern, Sean, Dennesen, Kristen, Feyes, Tonya, "Strategic Cyber Intelligence" *Information & Computer Security*, Vol. 23, No. 3, 2015, pp. 317-332. See also, INSA, Strategic Cyber intelligence, 2014, pp. 1-16 accessed 1 September 2017 at https://www.insaonline.org/strategic-cyber-intelligence/.

7. Brantly, Aaron F., *The Decision to attack. Military and Intelligence Cyber-Decision Making*, (Athens GA: The University of Georgia Press, 2016), Ch. 7, pp. 103-108 and 116-121.

8. Caligiuri, Mario, (2016), *Cyber Intelligence. Tra libertà e sicurezza* (Roma: Donzelli, 2016), Id., "Cyber intelligence, la sfida dei data scientist", June 2016, accessed 1 September 2017 at https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/cyber-intelligence-la-sfida-dei-data-scientist.html,

9. "Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry", Brussels, 2016, OJ C 75, 10.3.2017, pp. 124-128, par. 2.2.2.

10. Council of the EU, "EU Cyber Defence Policy Framework, Brussels", 18.11.2014, pp. 7, accessed 1 September 2017 at https://ccdcoe.org/sites/default/files/documents/EU-141118-EUCyberDefencePolicyFrame.pdf.

11. CERT-UK, "Integrating Threat Intelligence. Defining an Intelligence Driven Cyber Security Strategy", 2015, at https://www.cert.gov.uk/wp-content/uploads/2015/03/CPNI_CONTEXT_CERT-Threat_Intelligence.pdf.

12. "Cyber Security Strategy for Defence" (English version), par. 8 accessed 1 September 2017 at https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf.

13. Den Boer, Monica, (2015), "Counter-Terrorism, Security and Intelligence in the EU: Governance Challenges for Collection, Exchange and Analysis" *Intelligence and National Security*, Vol. 30, 2015, pp. 402-419.

14. ENISA, Big Data Threat Landscape and Good Practice Guide, January 2016, accessed 1 September 2017 https://www.enisa.europa.eu/publications/bigdata-threat-landscape.

15. ENISA, Threat Landscape Report 2015, Ch. 2.1; Threat Landscape Report 2014, Ch. 2.4.

16. ENISA, Threat Landscape Report 2016 15 Top Cyber-Threats and Trends, January 2016, Ch. 2, accessed 1 September 2017 at https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016. This product is the fifth in a series of reports analysing cyber-threats.

17. ENISA & RAND Europe, "Incentives and Challenges to Information Sharing", 2010, accessed 1 September 2017 at https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing.

18. Eom, Jung-ho, "Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace" *International Journal of Software Engineering and Its Applications* Vol. 8, No. 9, 2014, pp.137-146.

19. EPSC Strategic Notes, "Building an Effective European Cyber Shield Taking EU Cooperation to the Next Level", Issue 24, 2017, p. 7, accessed 1 September 2017 at https://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf.

20. EU Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN(2013) 1 final, Brussels, 7.2.2013, p. 10 and 17.

21. "Estrategia de Ciberseguridad Nacional 2013", p. 31, accessed 1 September 2017 at http://www.lamoncloa.gob.es/documents/20131332 estrategiadeciberseguridadx.pdf

22. Gori, Umberto, Germani, Luigi S., (2011), *Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia* (Bologna: Franco Angeli 2012).

23. Gruszczak, Arthur, (2016), *Intelligence Security in the European Union. Building a Strategic Intelligence Community*, (London: Palgrave-McMillian, 2016).

24. Helm, Stephanie "Intelligence, Cyberspace and National Security", EMC Chair Conference paper, accessed 1 September 2017 at https://www.usnwc.edu/ Academics/Faculty/Derek-Reveron/Workshops/Intelligence,-National-Security-and-War.aspx.

25. Hurley, Matthew M., "For and from Cyberspace Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance" *Air & Space Power Journal*, Vol 26, No. 6 (2012), pp. 12-33.

26. INSA, Cyber Intelligence: Setting the landscape for an emerging discipline, 2011, pp. 1 – 20, accessed

27. INSA, Operational Levels of Cyber Intelligence, September 2013, pp. 1-14, accessed 1 September 2017 at https://www.insaonline.org/operational-levels-of-cyber-intelligence/.

28. INSA, Tactical Cyber Intelligence, 2015, pp. 1-16 accessed 1 September 2017 at https://www.insaonline.org/tactical-cyber-intelligence/.

29. INSA, Operational Cyber Intelligence, 2015, pp. 1-16 accessed 1 September 2017 at https://www.insaonline.org/operational-cyber-intelligence/.

30. Kime, Brian P., (2017), "Threat Intelligence: Planning and Direction", accessed 1 September 2017 at https://www.sans.org/reading-room/whitepapers/ threats/threat-intelligence-planning-direction-36857.

31. Lee, Robert M., (2014), "An Introduction to Cyber-intelligence", accessed 1 September 2017 at https://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/;

32. Lee, Robert M., "Cyber Intelligence Collection Operations", 2014, accessed 1 September 2017 at https://www.tripwire.com/state-of-security/security-data-protection/cyber-intelligence-collection-operations/.

33. Ludwick, Melissa K., Townsend, Troy, Downing, Joan P., "White Paper – CITP Training and Education", Sep 2013, 6.1-6.24, accessed 1 September 2017 at http://www.sei.cmu.edu/about/organization/etc/upload/whitepaper.pdf.

34. Månsson, Kristofer, (2015), "Why cyber should not be limited to cyber, in Business Reporter", May 2015, accessed 1 September at https://business-reporter.co.uk/2015/05/31/why-cyber-should-not-be-limited-to-cyber/.

35. Montecillo, Michael, (2014), "Why Context is King for Enterprise IT Security", April 2014 accessed 1 September 2017 at https://securityintelligence.com/enterprise-it-security-context-king/.

36. "National Cyber Security Strategy 2. From awareness to capability" (English version), Annex I, Objective 1, Action No. 1, accessed 1 September 2017 at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf.

37. Office of the Director of National Intelligence, "The National Intelligence Strategy of the United States of America", 2014, pp. 1-24, accessed 1 September 2017 at https://www.dni.gov/files/2014_NIS_Publication.pdf.

38. Phythian, Mark (Ed.), *Understanding the Intelligence Cycle* (London and New York: Routledge 2013).

39. Regulation (EU) 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, Strasbourg, in OJ L 165/41, 18.6.2013, pp. 41-58.

40. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, Strasbourg, in OJ L 135, 24.5.2016, p. 53-114.

41. Sistema di Informazione per la Sicurezza della Repubblica, "Glossario Intelligence", December 2013, accessed 1 September 2017 at https://www.sicurezzanazionale.gov.it/sisr.nsf/quaderni-di-intelligence/glossario-intelligence.html.

42. UK MoD, "Joint doctrine publication 2-00, understanding and intelligence support to joint operations", JDP 2-00, 2011, accessed 1 September 2017 at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf.

43. US Department of Defense Science Board, "Resilient military systems and the advanced cyber threat", January 2013, pp. 46 and 49, accessed 1 September 2017 at http://www.dtic.mil/docs/citations/ADA569975.

44. US Department of Defense Science Board, "The Department of Defence Cyber Strategy", April 2015, p. 24 accessed 1 September 2017 at https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

45. Teti, Antonio, (2013), "Cyber Intelligence e Cyber Espionage. Come Cambiano i Servizi di Intelligence nell'era del Cyber Spazio" *Gnosis. Rivista Italiana d'Intelligence*, Vol. 3, 2013 pp. 95-121;

46. The UK National Cyber Security Strategy 2016-2021, par. 4.16, 5.0.2, 6.2.5 accessed 1 September 2016 at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

47. "The National Security Strategy and Strategic Defence and Security Review 2015. A Secure and Prosperous United Kingdom", par. 4.107 and 4.114 accessed 1 September 2017 at https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015,

48. Townsend, Troy, Ludwick, , McAllister, Jay, Mellinger, Andrew O., Sereno, Kate A., "Cyber Intelligence Tradecraft Project: Summary of Key Findings", the Software Engineering Institute (SEI) Emerging Technology Centre at Carnegie Mellon University, September 2013, pp. 2.01-2.20, spec. 2.5 at http://www.sei.cmu.edu/about/organization/etc/citp-summary.cfm. The full report is available at http://www.sei.cmu.edu/about/organization/etc/citp.cfm.

BIG DATA ANALYSIS THROUGH THE LENS OF BUSINESS INTELLIGENCE – WORLD CONFLICT INCIDENTS CASE STUDY (1989-2016)

Adrian BARBU [*]

Tudor RAȚ [**]

Abstract

Data analysis as a process and the specialized tools exploited in this regard, represent a powerful "weapon" available to anyone who wants to explore datasets, even for personal goals. The top business companies around the world are highly linked and dependent on the outputs revealed by the experts who manipulate various types of data on two coordinates: development and improvement; limitation of risks and vulnerabilities. Data analysis is not the perquisite of business branch; it is also intensively used by the intelligence agencies, mostly in areas like SIGINT or OSINT. Nowadays, data analysts are required to handle an enormous amount of data, which in many cases represents the biggest challenge for them and inferentially for the analytics. The technological evolution entails a capacity of rapid reaction to continuous transformation of data flows and the ability to conserve an accurate manner of sense-making in order to be able to provide useful data-based intelligence.

Keywords: *data, analysis, intelligence, interactive, visuals, forecast*

What is data analysis?

A report developed by Forbes Insights and Ernst & Young, shows that almost two-thirds of companies[1], which have well-developed analytics strategies and are using advanced tools of data analysis raised their profits by 15% in 2016. Technology and telecommunications are the two industries that are using with prepostency this type of tools. Companies and organizations that based their business activity on data analysis strategies, reveal that the

[*] Expert from Romanian Intelligence Service
[**] Expert from Romanian Intelligence Service
[1] 1,518 companies across a range of industries

ability of those who extract, manipulate and interpret datasets improved the competitiveness of the organization (Forbes Insights, 2017).

The advent of technology and the enormous amount of data which flows through the IT&C infrastructure requires specific methods, techniques and tools to capitalize collected data. The new era that provides a huge flow of various types of data advanced innovator concepts of analysing smaller or bigger datasets and shows us that we can use data as a strategic asset. This kind of approach supports the management department in identifying trends, opportunities, vulnerabilities and risks.

The business area views data analysis as a systematic operation of processing and shaping raw data, to sight out evaluations and to carry out logical inferences in order to frame analytical conclusions.

Data analysis is based on statistics and its focus relies on the relationships between variables. It is a widely used method in many fields (economy, marketing, sociology, intelligence etc.) because it delivers long-range insights about a specific problem taking in account large datasets.

In terms of intelligence activity, data analysis is mostly viewed as a sub-component of intelligence analysis and it refers to applying a set of cognitive methods to assess data and to test hypotheses. The result can be used as self-contained analytic product or it can be embodied in a comprehensive analytical framework.

Working with data implies both advantages and disadvantages. One of the most important benefits consists in summarizing large quantities of information, visualizing them in a graphic format and extracting the informational crux. Besides the measurements and the statistical feature, it is very important to use the proper visual tools to facilitate the assessment of the output data, because for the human brain is easier to understand the whole quantity of information presented in a chart or diagram. When the conclusions are extracted on a visual basis, the process will evolve fluently (Chen et al., 2011, p. 85).

Data analysis could also be productive in: identifying connections between entities, phenomena and processes; identifying typologies of entities, phenomena and processes; assessing and predicting the evolution of entities, phenomena and processes which were analysed; validation/ invalidation of various hypotheses; supporting the decision act by delivering information in a timely manner; identifying vulnerabilities or dysfunctions (Eising, December 1, 2010).

Dealing with a colossal amount of data sweeps out various challenges for those who manipulate datasets. One of the biggest problems in managing the datasets in a proper way, in order to analyse them, is related to the

foregoing step of analysis - the processing. It is a time-consuming activity, and the analysts should have the capacity to carry out the trimming, refinement and structuring of datasets in a timely manner. Another inconvenience is related to difficulties of interpreting numerical data, especially because the analysts have to think in a comprehensive way and correlate the numerical data with different other complex facets of the subject analysed.

Big Data and its 3 Vs

Data is generated with a high rate of velocity in every moment. All the processes made *via* the IT systems produce mostly unstructured data and the analysts must possess a complete set of skills to be able to manage these disparate flows, in order to reduce or to cut out the noise. By "Big Data" we should understand a complex concept which encompasses the techniques to capture, process, analyse and visualize mammoth datasets in a reasonable timeframe which cannot be achieved through standard IT technologies (Mukherjee, Shaw, 2016, p. 2).

According to Douglas Laney[2], the concept of "Big Data" is defined by three major elements:

- volume – collected data originates from a variety of sources (business transactions, social media, machine-to-machine data);
- velocity – large amount of data streams with higher and higher speed and must be dealt in a timely manner;
- variety – input data is collected in all types of formats (text, video, photo, audio in unstructured, semi-structured or structured databases) (SAS Analytical Solutions, 2017).

Big Data analysis, as well as the analysis of smaller datasets can reveal descriptive, predictive and/ or prescriptive insights about entities, phenomena or processes. Each type of outlook can be summarized in a question which defines the main purpose of the insight:

1. descriptive – "what happened in the past?";
2. predictive – "what might happen next?";
3. prescriptive – "how do I deal with this?" (Su, 2017, pp. 5-6).

The mentioned analysis methods were developed and used long time before the concept of Big Data. Although, the characteristics of the "new era of data" have shown the usability of analytics in delivering fast and actionable insights for the decision-makers providing both an early-warning tool and a well-developed instrument for the stakeholders.

[2] VP and distinguished analyst, chief data officer at Gartner

Cognitive biases in data analysis

Regarding the role of cognition in data analysis John Wilder Tukey stated: "The basic general intent of data analysis is to seek through a body of data for interesting relationships and information and to exhibit the results in such a way as to make them recognisable to the data analyser. [...] At all stages of data analysis the nature and detail of output, both actual and potential, need to be matched to the capabilities of the people who use and want it" (Wilder Tukey,1962, pp. 1-67).

All types of analyses rely on the ability of human mind to interpret and assign meaning to the collected and processed data, usually in accordance with a specific context or goal.

Foregoing the analytical process, a logical plan and a sense making schema should be developed, in order to avoid or to limit the cognitive biases. Commonly, there are four main types of biases that darken the analyst's judgement during the operation with large datasets.

The first one is the confirmation bias which refers to the need of proving a hypothesis. The analyst tends to lean on data that might certify the initial assumption. In this case, the full picture of the scenario might be left out, because the analysed data does not represent the relevant information (Smyth, July, 2017).

The second main type is the sampling bias, also known as selection bias. Occasionally, the available timeframe for the requested analysis is limited and one needs to extract a sample from the entire amount of data. The sampling procedure is usually achieved by applying a range of statistical techniques and a well-designed randomization. Errors may appear if the sample is not representative for the whole dataset that will be analysed (Crawford, Kate, April 1st, 2013).

The third one is related to the illusory correlations made between data variables. This bias occurs when a correlation between two variables is detected when no relationship actually exists. Also, this could evolve in connecting a cause to an effect even when there is no link between them (Grisanti, April 30, 2015).

Last but not least, the so-called *apophenia* is the tendency of humans to see patterns in randomness. This cognitive bias, similar to the previous one, may occur when people identify connections between meaningless data, usually due to the lack of expertise and experience (Grisanti, April 30, 2015).

The human resource cannot be removed from the process of analysis, hence the cognitive biases will linger and the analysts need to be aware of the errors that might shadow the output. In order to thwart blundering interferences in the judgment process, there are a couple of actions that could

limit the cognitive biases: collect data from as many points as possible, even if they seem irrelevant at first glance; create clear and structured datasets, free of subjectivity; maintain an impartial behaviour in manipulating datasets.

Likewise, analysing Big Data by using business intelligence (BI) specialized tools represents a proper way to avoid cognitive biases. This type of technological solution does not deliver only descriptive information based on the available datasets; it also uses strong mathematical algorithms which can provide accurate forecasts useful in the process of testing hypotheses.

Case study – conflict incidents 1989-2016

As was mentioned above, data analysis is a valuable asset in pointing out patterns and future developments of an event or phenomenon. Armed conflicts have always been one of the biggest threats for the national, regional and global security. Even more, nowadays the governments are facing multiple issues regarding conflict prevention and conflict management. Wars are now worn mostly between state and non-state actors and the strategies, tools, and tactics used by rebels, paramilitary groups, terrorist or any other non-state entities have changed in such way that classic counter-measures have become useless.

Using *Tableau*, a business analytics service and interactive data visualization tool[3], a scientifically validated dataset[4] comprising the armed conflicts between 1989 and 2016 (excluding Syria) and the associated variables were explored in order to develop relevant analytic conclusions that might help in subsequent investigations on this subject (UCDP Conflict Encyclopedia).

The focus of the analysis was on two main components:

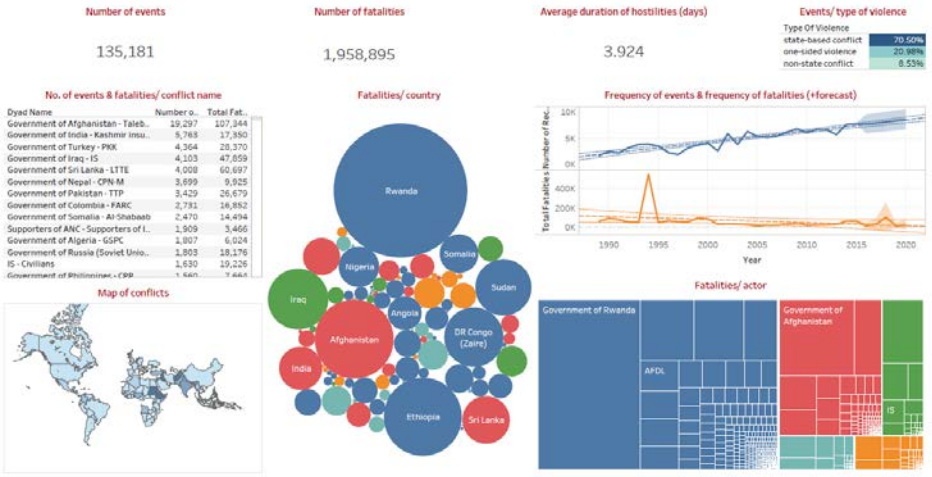
- number of events and fatalities in terms of country, region and actors;
- frequency of events and fatalities and possible evolutions.

[3] Tableau puts analytics in the hands of the user. By enabling individual creativity and exploration from the ground floor, businesses now the ability to adapt and outperform competition through intuitive data visualization and analysis. Tableau can connect to virtually any data source, be it corporate data warehouse, Microsoft Excel or web-based data. It gives users immediate insights by transforming their data into beautiful, interactive visualizations in a matter of seconds. What took expensive teams days or months to develop now is achieved through the use of a user-friendly drag-and-drop interface.

[4] The UCDP Conflict Encyclopedia (UCDP database) is an online, free of charge, database. It is updated and revised several times per year and contains detailed descriptive information on armed conflicts, peace agreements, and several other aspects of organised violence. Coverage is global with information from 1946 and onwards.

One of the issues that we need to be aware of from the beginning is that we deal with a heterogeneous dataset. The standard deviation of the variables shows that the values are spread out and characterized by irregularity. This means that values associated with various conflicts, like fatalities and incidents are far-off from the average. The best example is that of the Rwandan genocide.

As we could notice, in a period of 27 years, there were 135,181 events[5] that generated 1,958,895 fatalities among the belligerents and also civilian population. 70,50% of the incidents were state-based conflicts, 20,98% one-sided violence and 8,53% non-state conflicts.



The conflict with the highest number of incidents was the Afghan Civil War (19,297), followed by the insurgency in the Kashmir region (5,763), Turkish Government - PKK conflict (4,364) and the conflict between the Iraqi Government and Daesh (4,103). However, the most violent conflict, in terms of fatalities, was the Rwandan genocide (511,531), followed by Afghan civil war (107,344), Eritrean-Ethiopian war (97,435), and Sri Lankan civil war (60,697).

On one hand, we can remark that the highest rate of fatalities has occurred in the African region, particularly in Rwanda, Ethiopia, Democratic Republic of Congo, Sudan, Nigeria and Somalia. On the other hand, the highest

[5] An event is defined by UCDP as an individual incident of lethal violence occurring at a given time and place.

rate of events is related to the Middle East and Far East conflicts, especially in Afghanistan, India, Nepal, Pakistan, Sri Lanka and the Philippines.

Last year (Jan-Dec 2016), most of the 53,954 victims (approximate 70%) were caused by the conflicts between terrorist groups/ Islamic fundamentalists and different governmental forces, with prepostency in Middle East and North Africa.

In terms of non-state conflicts, the hostilities were the most active in South Africa, between the supporters of Inkatha Freedom Party and the supporters of African National Congress[6]. There is a big variety of actors related to this type of conflict, from partisans of different political parties or political movements[7], organized crime groups[8] and various ethnic or religious communities, to terrorist and radical Islamic organizations[9]. It is also noticeable the disposal of the type of actors by continents and regions: supporters of opposing political organizations in Africa, organized crime groups and urban guerrillas in Latin America and terrorist groups in Middle East and North Africa.

Conclusions

Visualising and analysing in an interactive manner this type of dataset, with more than 130,000 entries, revealed useful insights regarding interstate and intrastate conflicts. The complex options of filtering, cross-filtering, easy capabilities of exploring and mathematical algorithms available in the BI tool allowed pattern identification and trend detection. The outputs could serve as a basis for future assessments on the evolution of specific violent incidents or the development of the whole phenomenon.

On the African continent, armed conflicts are more violent than in any other part of the world, even if there were fewer events, compared to Middle East and North Africa where the number of incidents was the highest. This is an essential mark of the characteristics of conflicts depending on the source region and it could be also useful in order to understand the particularities of the societies involved.

As non-state actors, the South American criminal organizations, paramilitary groups and the Islamic jihadists produced over 9 out of 10

---

[6] 1,909 incidents; the second non-state conflict with the highest rate of events was the conflict between Juarez Cartel and Sinaloa Cartel

[7] e.g. United Democratic Front (India), National Socialist Council of Nagaland, Muhajir Quami Movement (Pakistan)

[8] e.g. Gulf Cartel, Sinaloa Cartel, Los Zetas, Tijuana Cartel

[9] e.g. Hezbollah, Al-Qaeda in Arabic Peninsula, Daesh

victims. The forecasted trend for this type of violence is heavily ascending. If we refer to ongoing state-based conflicts, the Afghan civil war is still the most "prolific" in terms of fatalities and number of incidents.

Regarding the frequency of incidents in the last years, after a narrowing trend from 2011 to 2013, we can observe a continuous escalation. Furthermore, the forecast tool predicts that the level will increase lineal at least until 2020.

With regard to the frequency of fatalities, there was a slow increase from 2013 to 2014, albeit the trend-line is descending since 1995. The number of victims will grow till 2018, followed by a decrease in 2019 and a slow increase in 2020.

References:

1. Chen, Min, Trefethen, Anne, Banares-Alcantara, Rene , Jirotka, Marina, Coecke, Bob, (2011), *From Data Analysis and Visualization to Casuality*, Washington: IEEE Computer Society.

2. Crawford, Kate, (April 1st, 2013), *The Hidden Biases in Big Data*, accessed 27 August 2017, https://hbr.org/2013/04/the-hidden-biases-in-big-data.

3. Eising, Martin, (December 1, 2010), *Data Analysis Overview*, accessed 15 August 2017, http://www.dashboardinsight.com/.

4. Forbes Insights, (2017), *Data & Advanced Analytics: High Stakes, High Rewards*, accessed 5 September 2017, https://insights.forbes.com/advanced-analytics-high-stakes-high-rewards/?aliId=88748382.

5. Grisanti, Julie, (2017), *Trust the Data: How to Counteract Human Cognitive Biases*, accessed 27 August 2017, http://www.aunalytics.com/trust-the-data/.

6. Mukherjee, Samiddha, Shaw, Ravi, (2016), *Big Data – Concepts, Applications, Challenges and Future Scope*, International Journal of Advanced Research in Computer and Communication Engineering, vol. 5, February.

7. SAS Analytical Solutions, (2017), *Big Data – What it is and why it matters*, accessed 6 September 2017, https://www.sas.com/en_us/insights/analytics/big-data-analytics.html.

8. Smyth, Daniel, (July, 2017), *Four cognitive biases that affect big data analysis*, accessed 27 August 2017, http://bigdata-madesimple.com/four-cognitive-biases-that-affect-big-data-analysis/.

9. Su, Xiaomeng, (2017), *Introduction to Big Data*, Norwegian University of Science and Technology, Trondheim.

10. UCDP Conflict Encyclopedia (UCDP database): www.ucdp.uu.se, Uppsala University.

11. Wilder Tukey, John, (1962), *The future of data analysis*, The Annals of Mathematical Statistics, Vol. 33, pp. 1-67.

BUSINESS COUNTERINTELLIGENCE PRACTICES

Horia Mircea BOTOŞ [*]

Gheorghe RADU [**]

Abstract

Counterintelligence, as defined by the Merriam Webster Dictionary, is an organized activity of an intelligence service designed to block an enemy's sources of information, to deceive the enemy, to prevent sabotage, and to gather political and military information. It protects against espionage, assassinations, etc. that might be done by a foreign agent. Likewise, when we think about business, the source of a country's wealth, Business Counterintelligence is an effort of an organization or country to protect its private and hypersensitive information from being unwantedly accessed.

Intelligence refers to the information that supports decision making and sustains strategic developments. Thus counterintelligence is the information used to defend the company from another competitive business and all the implied tools and processes.

Because of this, Competitive intelligence and Business Counterintelligence are considered sometimes synonymous, despite being different. Competitive intelligence is the gathering of information, whereas business counterintelligence is the protecting of the information against the CI efforts. So business counterintelligence represents the actions taken to limit the access of others to the sensitive and actionable information of the company.

In this paper we will identify and structure the term of business counterintelligence and will present examples of such practices. We will try exemplifying the use of counterintelligence in the business sector by presenting, from a theoretical point of view, the Russian approaches on Western companies.

Keywords: *Intelligence, Counterintelligence, Business Intelligence, Business Counterintelligence, Russia*

Theoretical aspects

Counterintelligence (CI) refers to information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations

[*] PhD, Babes Bolyai University DSIIC horia.botos@gmail.com

[**] BA Security Studies, Babes Bolyai University DSIIC, gicu.radu1@gmail.com

or persons or international terrorist activities, but not including personnel, physical, document or communications security programs. [1]

When we speak about *counterintelligence* we should know that this term is divided in three main categories:[2]

1. *Collective counterintelligence* – is responsible for gaining information about an opponent's intelligence collection capabilities whose aim is at an entity.

2. *Defensive counterintelligence* – the thwarting efforts by hostile intelligence services to penetrate other services.

3. *Offensive counterintelligence* – the action of identifying another opponent's efforts against the system, trying to manipulate these attacks by either "turning" the opponent's against into double agents or feeding them with false information.

Also this term is used in more spheres. When we speak about *military counterintelligence,* we should go with our mind to the United Stated Army Counterintelligence that is responsible for the *counterintelligence* activities aimed to detect, identify, assess, counter, exploit and/or neutralize adversarial, foreign intelligence services, international terrorist organizations, and insider threats to the United States Army and U.S. Department of Defence.[3]

We also have *economic counterintelligence.* A good example here is the program initiated by FBI in 1994 which was created to protect the U.S. national security. Kenneth Geide that was the head of the Economic Counterintelligence Unit, explained that one of the methods that foreign governments often use is to hide their economic collection activities within their legitimate activities.[4]

Because of this nature of the Counterintelligence service, it offers a wide array of tactics, techniques and protocols that insure a company's Information security. Such services may include: analysis of vulnerabilities for specialized threats (internal and external to the company), Business operational procedures, Proprietary Information Protective measures, Research and analysis of offensive Business Intelligence Practices.

Business intelligence (BI) refers to the procedural and technical infrastructure that collects, stores and analyses the data produced by a company's activities. Business intelligence is a broad term that encompasses

---

[1] Executive Order 12333. (1981, December 4). United States Intelligence Activities, Section 3.4(a). EO provisions found in 46 FR 59941, 3 CFR, 1981 Comp., p.1

[2] Lowenthal, M. (2003). Intelligence: From secrets to policy. Washington, DC: CQ Press.

[3] United States Army Regulation 381-20, *The Army Counterintelligence Program*, May 25, 2010

[4] Hedieh Nasheri, Economic Espionage and Industrial Spying, p76

data mining, process analysis, performance benchmarking, descriptive analytics, and so on. Business intelligence is meant to take in all the data being generated by a business and present easy to digest performance measures and trends that will inform management decisions.[5]

Business counterintelligence (business CI) is the collective efforts designed to protect an organization's sensitive information from unauthorized access.[6]

Taking in consideration this definition of Business counterintelligence, we can observe that it is similar to the one of Competitive Intelligence (The process of collecting and analyzing information about competitors' strengths and weaknesses in a legal and ethical manner to enhance business decision-making). Competitive intelligence is the activity responsible for gathering information, whereas business counterintelligence is the activity responsible for the protection of the information against the Competitive Intelligence efforts. So *business counterintelligence* represents the actions taken to limit the access of others organizations to important information that could put the company at a disadvantage if made public. Such information could be: R&D developments, future investments, intellectual property information or M&A's.

Functions and Forces defining Counterintelligence

Our study has evidenced that the general functions in the field of Counterintelligence remain the same regardless of the field of application. The fields of from the perspectives of which the analysis would be are: technological, economic, occupational, spatial and cultural.

The four functions of CI are:

a) operation;
b) investigation;
c) collection and reporting;
d) analysis, production and dissemination.

The CI Operations employ specialized techniques and personnel, and are directed against any espionage, sabotage, subversion or threats. As directed to general activities, Business Counterintelligence covers: counterespionage, counter subversion, counter sabotage and exploitation or neutralization operations. Compared to standard CI, you can observe that there are no mentions of terrorism, as this is generally a referred as unlawful use of violence and intimidation of civilians, in principal, in order to follow a political aim.

---

[5] http://www.investopedia.com/terms/b/business-intelligence-bi.asp
[6] Business Counterintelligence : Sustainable Practice Or Passing Fad?, Shear, Christopher James, accessed at: http://scholar.sun.ac.za/handle/10019.1/1930

CI investigations are the next function, and they cover systematic and detailed inquiries/examination to uncover facts on the matter that is the objective of the operation. The results of these actions are the function of Collection and Reporting, which are intended to identify actual or potential threats. After these functions are done, the next function will be the performing of an analysis on the available data and information, producing the report and afterwards handing in the results.

In Business CI, the protocol is not far off; just the purpose is aligned with the Business needs of an organization in order to protect itself from its competitors. This is why when analyzing the academic materials on Business Counterintelligence you will find many mentions of corporate espionage or corporate counterespionage.

The perspectives initially mentioned are just some of the elements that customize Business Counterintelligence so that the CI protocols are corporate oriented. The technological perspective makes technology look like an important factor, which is a societal structure that leads to the reforming of such projections of the information society. This is stemmed from the idea of conflict innovation, which is resulted ideology since the period the Cold War started. It has extended to the business form the military form, Sputnik theory being an example of this.

The economically founded perspective is where the information is seen as a factor of the Gross National Product within the economy, and thus influencing market development for the private corporations. Because of this Business Counterintelligence data will refer to quantitative and qualitative aspects of the economic factors.

The occupationally force is where the occupational structure is patterned and analyzed as part of the informational work activities.

The spatial force is referring to the perspective of the geographical point of view and places the procedure organization on the digital map and determines an informational flow within the existing networks. There are variously disparate spatial entities that can be connected between themselves and thus confirming that the organizations is part of the information driven social organization.

The cultural perspective defines itself on the idea that the social conception has given the organization an increase of information availability within information societies. One of the advantages brought is the increase in types and channels of information available.

We have to take into consideration that the multifaceted nature of business intelligence forces the organization to structure a framework in order to maximize the results of their actions. These 5 mentioned perspectives will give companies the possibility to put into action the four functions in a

way that will maximize the protection received by them from unwanted and unauthorized access.

Cyber-crime and Business Counterintelligence

Eoghan Casey defines *Cyber-crime* as an infraction that involves a computer used in the commission of the crime, or represents the main target of this crime, and a network.[7] This notion can be divided in some subcategories:

a) Fraud and financial crimes;
b) Cyber warfare;
c) Cyber extortion;
d) Cyber terrorism;
e) Computer as a target;
f) Computer as a tool.

A resounding case of *Cybercrime* based in Russia was discovered in 2006. It references an internet site named Russian Business Network (RBN), and its administrator that shortly after its opening discover that he can earn a lot more money by hosting illegitimate activities. So he started to offer web hosting services to all kinds of criminal and objectionable activities, earning more than $150 million in one year.[8]

In recent years we have witnessed a rise in Cybercrimes and in 2017 we have had the largest cyber-attack in current history. The first was called WannaCry, started in May 12, and it cashed 52 Bitcoin ($ 130.000). At about a month later a second attack took place, Petya, it was more advanced the WannaCry, but is had an ineffective and inefficient payment system. Petya disrupted utilities like power companies, airports, public transport or central bank.

In order to stop cyber-attacks and cyber-crimes developments in the cyber-security field have advanced by in both public and private sectors. After the 9/11 attack, national agencies have registered a rise in the investigation and invest of cyber-attacks, in order to create an international infrastructure of fighting terrorism. This infrastructure consists of state organizations, private companies and universities, which develop cutting-edge research and developments. The development of the investigation capacities of the Cyber divisions is focused on the intrusions into government and private computer networks of information, destined to steal intelligence.

Because of this, Business Counterintelligence with the before mentioned functions and perspective, is oriented to determine and understand the behaviour and psychological reasoning for the attacks. Further

---

[7] Robert Moore, "Cybercrime: Investigating High-Technology Computer Crime" (Anderson Publishing, 2011), p.4

[8] The Economist, http://www.economist.com/node/9723768 accessed 29 august 2017

in the paper we will describe the Business Counterintelligence in case studies from different countries from around the world.

Case study – manifestations of Business Counterintelligence around the world

In this part of our work we will try to present some examples of *Business Counterintelligence manifestations*, and how are they used by "Big Powers" to influence the international politics.

Firstly, we will speak about Russia, one of the biggest powers until 1990, and an important actor on the international political scene nowadays. Russia has two main companies that are used to change or to blackmail other countries decisions. Even president Vladimir Putin noted that "these companies are very real and each year are accumulating more and more wealth and international influence, which they are using to advance the interests of the Russian state."[9] I think most of you already know that we will talk about "Gazprom" and "Rosneft".

Gazprom is considered an important "weapon of diplomacy" used by Russia because of its importance on the international arena. In the early 1990s, after the fall of the Soviet Union, Russian administration decided to privatize the previously state-owned businesses for being able to create a free-market economic system. This company was an exception, because the Ministry of the Gas became now a corporation named Gazprom, where the state owned more than 50% of actions.

President Putin talked in his work "Mineral and Raw Materials Resources and the Development Strategy for the Russian Economy." about the importance of this new company, and after 1999, Russian started to hire former secret and special services agents as high ranked workers in Gazprom. Even more, some oligarchs and State Duma members suspected than the corporation will be favoured by the president and his administration who wanted to monopolize the energetic sphere. Years later these suspicions have come true when "Yukos" that once was the world's largest nonstate oil company was completely dismantled, or when Shell lost its controlling stake over Sakhalin 2 project through highly questionable methods.[10]

Another "favour" is made after 2006 when the Russian state changes the rules in favour of big companies and gives them full control over their territory and the possibility to equip their "army" with firearms and UAV's produced in Russia or Israel for being able to prevent sabotage, hijacks,

---

[9] Marshall I. Goldman, Petrostate: Putin, Power, and the New Russia (United Kingdom: Oxford University Press, 2008), p.3

[10] Cindy Hurst, The Militarization of Gazprom, September - October 2010, p61, accessed 28 August 2017, http://www.dtic.mil/get-tr-doc/pdf?AD=ADA529212

hostage situations etc. Gazprom security service was employing more than 20000 men, who were responsible for body-guarding, intelligence and counterintelligence, plant protection, and transport of valuables, and were paid with a salary that was five or six times bigger than a security state worker salary. During the years, Russia used Gazprom to blackmail the European countries or ex-soviet states to maintain their regional influence. The most used method by Gazprom is the price raising or cutting the natural gas supply.

Such cases where reported in 2004 when Russia stopped the gas that was passing through the "Drujba" pipe to Latvia. This action was taken to encourage the privatization of Latvian companies that imported petroleum by the Russian oligarchs. Also in 2006 they stopped the gas going to Ukraine because of its "debts", or they threatened Georgia to halt supplies if they will not accept the new gas price that was 2 times bigger than the old one, and also bigger than the price proposed for other states. Of course we should not forget about its intermediaries that are more than 50 in the whole Europe, and are used to serve their own interests. Such a cases were present when Gerhard Schröder an ex-German canceler was named as Gazprom CEO, after he signed an agreement with this company that raised the Germany dependence on Russian gas, or when a audio recording between the polish oligarch Marek Dochnal and the Russian agent Vladimir Alganov where they were discussing about the privatization of the polish energy industry.

In conclusion, starting from the general definition of *Business Counter Intelligence*, we can observe that Russian officials with the Gazprom administration have undertaken a series of security measures to protect their sensitive information and interests from unwanted intruders that can harm them or their state and can alleviate their influence in the international scene.

Rosneft has a little different story. It is a company that always managed to have important contracts with foreign partners such as ExxonMobil who wanted to participate at the petroleum extraction in Siberia, or British Petroleum who signed a $1.5 billion contract for the import of 12 million tons of petroleum products.[11] Here we have a direct favoring attitude from the Russian state, or its administration, with Andrei Patrushev the son of Nicolai Patrushev (former FSB chief and Security Council) and their CEO Igor Sechin, an ex-secret agent are used to "swallow" their competitors by starting criminal proceedings against them. A good example is the case with Vladimir Evtushenko, the CEO of "Bashneft" who was forced to yield his company,

[11] *Adrian Stoica, "CONTRACTE DE MILIARDE DE DOLARI: Apetitul pentru hidrocarburile rusesti si sanctiunile economice", accessed 29.09.2017, http://www.petroleumreview.ro/ro/29-iulie-augusr-2014/190-contracte-de-miliarde-de-dolari-apetitul-pentru-hidrocarburile-rusesti-si-sanctiunile-economice*

losing $7.2 billion. After this he will be forced to pay $2.3 dollars this amount exceeding his wealth. [12]

Another proof for how important is Rosneft for president Putin is the case with the privatization of 19.5% of the company. Officially, these actions were bought by Qatar, Glencore and the Italian bank Intesa Sanpaolo, making abstraction from the EU sanctions. Analysts say that this was a political move, to show the world that even with the EU sanctions, there are countries who trust Russia and believe in its stability. After some investigations it turned out that the real buyers were not Qatar, Glencore or Intesa Sanpaolo. The only thing that is known is that money and actions passed through some phantom companies from Cayman and Singapore, but nobody is ready to offer more details.[13]

Now, speaking about the western part of the world, we will analyse Royal Dutch Shell and ExxonMobil, two very important oil and gas companies.

First of all, we mentioned the case about Shell and Sakhalin 2, a project that includes development of the Piltun-Astokhskoye oil field and the Lunskoye natural gas field offshore Sakhalin Island in the Okhotsk Sea, and associated infrastructure onshore.[14] In that period, the company was indirectly forced to sell its part of actions to Gazprom. Despite of these, in 2015 Shell started new negotiations with Russia for new projects that will cost more than $11 billion, even if Russia had a list of sanctions imposed by Europe and USA. Making abstraction from the fact that both of them will make a lot of money from this contracts, Royal Dutch Shell can be viewed as an instrument used to "control" in some limits to monitor the activity of Gazprom, their real plans and the way they work.

ExxonMobil, which is considered the largest of the world's Big Oil companies[15] always was in good relations with Rosneft because of their common profitable activities. An example can be their agreement signed in 2011 when Exxon was allowed to conduct offshore exploration in the Black

---

[12] Catalin Apostoiu, "De ce Rosneft, cea mai mare companie petrolieră a Rusiei, câştigă mereu", accessed 29.09.2017, http://www.zf.ro/business-international/de-ce-rosneft-cea-mai-mare-companie-petroliera-a-rusiei-castiga-mereu-16707949

[13] Bogdan Cojocaru, "Privatizarea Rosneft, promovată de Moscova ca un vot de încredere din partea investitorilor străini, este îngropată adânc în mister", accessed 29.09.2017, http://www.zf.ro/business-international/privatizarea-rosneft-promovata-de-moscova-ca-un-vot-de-incredere-din-partea-investitorilor-straini-este-ingropata-adanc-in-mister-16121643

[14] Miriam Elder (2008-12-27). "Russia look to control world's gas prices". Telegraph. Retrieved 2008-12-27.

[15] "FT's profile of ExxonMobil". *Financial Times*. Retrieved April 21, 2008.

Sea and the Kara Sea in Siberia.[16] There were cases when the company violated sanctions on Russia in the period when actual secretary of state Rex Tillerson was the CEO. In 2017 The Treasury Department of USA fined Exxon Mobil $2 million, which is not a significant punishment for this "mammoth".[17] Some experts consider that the good business relations between Mr. Tillerson and Mr. Sechin are responsible for this violation and were reflected in the 2016 presidential elections in USA. Now, if this was just a small part of what "business relations" can do, we can imagine what will happen in a few years.

Conclusions

Intelligence theory has shown us that it has two main sections. The first one the Business/Competitive Intelligence that is working for the company in order to find information that helps it develop. The second is Business Counter Intelligence, which protects the company from any factor that can give its competitors a development advantage over it.

As our examples showed, Business Counter Intelligence has been used by companies and states in order to protect their economic interests. Especially in the case of Russia, which is known for being a state that uses Intelligence practices in order to protect its interests, they have used may of the practices mentioned in the article in order to protect the country from any disruptive action towards the countries mineral resources. As Russia is the world leader in exporter of energy resources (crude petroleum, refined petroleum, gas and coal[18]), this has always been a sensitive matter.

Such practices are common with other countries, as the U.S.A, Peoples Republic of China, India or Germany, Russia's Government action were always visible specially with the help of the defectors that explained their tactics.

This extensive use of Business Intelligence and Counter Intelligence are widely known, but the fast moving age of information in which we live in, has made it even more relevant for a company or state to control and maximize the use of the available resources.

---

[16] Donna Borak and Matt Egan, "Trump denies Exxon permission to drill for oil in Russia", CNN Money, retrieved April 21, 2017. Accessed 05.09.2017 , http://money.cnn.com/2017/04/21/news/companies/trump-exxon-russia-sanctions/index.html

[17] Alan Rappeport, "Exxon Mobil Fined for Violating Sanctions on Russia", The New York Times, accessed 05.09.2017, https://www.nytimes.com/2017/07/20/us/politics/exxon-mobil-fined-russia-tillerson-sanctions.html

[18] http://atlas.media.mit.edu/en/profile/country/rus/

This military practice that passed into the civilian zone, has shown the development of the strategic capabilities into a powerful decision making tool. Despite the fact that Counter intelligence is a military protocol, its civilian business oriented variation has demonstrated itself as effective.

Please keep in mind that, due to the nature of Intelligence, Business Counterintelligence will always have a restrictive character from the point of view of an academic, as the detailed aspects addressing its protocols and best practices will be kept as private as possible. Keeping this in mind and thinking about the functions and forces affecting Business Counterintelligence, we can conclude that there is no specific "receipt" to put this process into action. We have saw the way in which it is performed by the Russians companies and what affects it had on their counterparts.

References:

1. Carlisle R., " Encyclopedia of Intelligence and Counterintelligence",2015, Routledge.
2. Cojocaru, Bogdan, "Privatizarea Rosneft, promovată de Moscova ca un vot de încredere din partea investitorilor străini, este îngropată adânc în mister", accessed 29.08.2017, http://www.zf.ro/business-international/privatizarea-rosneft-promovata-de-moscova-ca-un-vot-de-incredere-din-partea-investitorilor-straini-este-ingropata-adanc-in-mister-16121643
3. "Counterintelligence – Best Practices for Cleared Industry ", 2014 , accessed 20.08.2017 at: https://cyberwar.nl/d/20141028_US-DoD-Counterintelligence-Best-Practices-for-Cleared-Industry_CIBooklet.pdf
4. Elder, Miriam, (2008-12-27). "Russia look to control world's gas prices". Telegraph. Retrieved 2008-12-27.
5. Goldman, Marshall I., Petrostate: Putin, Power, and the New Russia (United Kingdom: Oxford University Press, 2008)
6. Harber, J.R., "Unconventional Spies: The Counterintelligence Threat from Non-State Actors", 2012, accessed15.08.2017 at: https://modularconstructionna. iqpc.com/media/6089/476.pdf
7. Hurst, Cindy, The Militarization of Gazprom, September - October 2010, accessed 28 August 2017, http://www.dtic.mil/get-tr-doc/pdf?AD=ADA529212
8. Michal K., "Business counterintelligence and the role of the U.S. intelligence community", 2008, International Journal of Intelligence and Counterintelligence Vol. 7 , Iss. 4, accessed 10.08.2017
9. Moore, Robert, "Cybercrime: Investigating High-Technology Computer Crime" (Anderson Publishing, 2011), p.4
10. "Protecting Key Assets: A corporate Counterintelligence Guide", DNI, accessed 22.08.2017 at: https://www.dni.gov/files/NCSC/documents/Regulations/ ProtectingKeyAssets_CorporateCIGuide.pdf

11. Stammberger, S., "GoogSpy: Business Counter Intelligence for Everyone", accessed 5.09.2017 at: http://www.intelligencesearch.com/ia048.html

12. Shear, C.J., "Business Counterintelligence: sustainable Practice or Passing Fad?", 2009 , accessed 15.08.2017 at: http://hdl.handle.net/10019.1/1930

13. US Marine Corps, "Counterintelligence – MCWP 2-6", 2016, accessed 22.08.2017 at: http://www.marines.mil/Portals/59/Publications/MCRP%202-10A.2%20(Formerly%20MCWP%202-6).pdf?ver=2016-06-01-135919-697

INTELLIGENCE ANALYSIS

HOW TO EXCEL AT INTELLIGENCE ANALYSIS

Davide BARBIERI [*]

Stefania PALADINI [**]

Abstract

Easy-to-use and commonly available software tools may significantly improve the way intelligence analysts do their job. This is especially true when quantitative assessments - which involve statistical and mathematical calculations - are required by decision makers. The possibility to chart and display results in an intuitive way will facilitate reporting and communication, minimizing ambiguities and the necessary narrative to make sense of collected information. This paper shows how to efficiently leverage MS Excel to produce elegant and accurate intelligence reports for early-warning tasks. As an example, information collected from social media is used in order to update coherently the estimates of the risk of a war between the USA and North Korea.

Keywords: *Electronic spreadsheets, social media, quantitative risk assessment, Bayesian inference.*

Introduction

The use of Bayesian techniques (Bayes and Price 1763) in security analysis is long established. They helped Alan Turing to break the Enigma code in WWII and the US Navy to track Soviet submarines during the Cold War. The Rand Corporation has used them extensively to assess the probability of a nuclear war. More specifically, some early attempts to quantitatively evaluate the risk of a conflict using software applications based on the rule of Bayes were made in the second half of the last century by the Central Intelligence Agency (Zlotnick 1970, Fisk 1972, Schweitzer 1976).

The technology adopted back then was expensive and not widely available, even though it had a limited working memory and processing capability. Subsequent progresses in digital electronics have determined

[*] PhD, University of Ferrara (Italy), davide.barbieri@unife.it

[**] PhD, Birmingham City University (UK), stefania.paladini@bcu.ac.uk

the widespread adoption of powerful computers for personal use. Modern PCs have much larger processing and storage capacities than those of mainframe computers used forty years ago. Moreover, cheap and user-friendly software - like electronic spreadsheets that can perform advanced mathematical and statistical calculations - have been extensively acquired by non-computer scientists.

Moreover, in the last ten years, a series of sophisticated tools, compounding Bayesian analysis with other quantitative methods, have been developed (Kardes and Hall 2005), such as: Bayesian Networks, Multi-Entity Bayesian Networks and Hidden Markov Models, generally adopted to evaluate asymmetric threats. Recently, a Bayesian approach has been proposed for intelligence analysis in general (Barbieri 2013), laying the foundations and epistemic premises for quantitative inference in the field. In addition, the same approach has been suggested for the risk assessment of violent extremisms (Barbieri and Pressman 2015).

Although Bayesian reasoning is often perceived as counter-intuitive, some successful efforts have been made to teach it to non-statisticians (Gigerenzer and Hoffrage 1995, Hoffrage and Gigerenzer 1998, Sedlmeier and Gigerenzer 2001), and in particular to intelligence professionals (Wheaton et al. 2009). The aim of this study is to evaluate the use of Microsoft Excel and the rule of Bayes for intelligence analysis for early warning tasks, in order to assess quantitatively the risk of a major conflict.

Method

The conditional probability of an event given some piece of information or evidence can be calculated using the rule of Bayes:

$P(H_0|E)= P(H_0)P(E|H_0)/P(E)$

where:

- $P(H_0|E)$ is the *posterior* or revised probability of H_0 (the starting or *null* hypothesis) given evidence E.
- $P(H_0)$ is the *prior* probability of H_0, or *base rate* (akin to *prevalence* in epidemiology). It is the first "bet", which must be stated explicitly before evaluating any information.
- $P(E|H_0)$ is the *likelihood* of observing E in case H_0 is true. In some cases, historical records can be used to assess it. This is the norm in medical diagnostics, where the rate of true positives of a medical exam is known. In early warning tasks, this is not the case and it must be subjectively estimated.

- P(E) is the probability of observing E regardless of which hypothesis is true, H_0 or H_1 (the alternative hypothesis). It can be calculated as $P(E)= P(H_0)P(E|H_0)+P(H_1)P(E|H_1)$. Therefore, also $P(E|H_1)$, the likelihood of observing E in case H_1 is true, must be estimated.

The rule of Bayes can be easily implemented in Excel. First, the two competing hypotheses must be stated explicitly in the top cells (as in Figure 1). Usually, the null hypothesis H_0 is that of no war, which was the actual situation at the beginning of this study. H_1 is the alternative hypothesis of an imminent war. There are no real caveats against using the opposite approach, with H_0 corresponding to war and H_1 to no war. Still, it is important that both hypotheses are declared explicitly, in order to avoid any misunderstanding.

Figure 1. The formatted Excel spreadsheet.

	A	B	C	D	E	F	G	H	I
1	H_0:	no war							
2	H_1:	imminent war							
3	Date	$P(H_0)$	$P(H_1)$	$P(E\|H_0)$	$P(E\|H_1)$	$P(H_0\|E)$	$P(H_1\|E)$	source	Evidence
4			=1-B4			=B4*D4/(B4*D4+C4*E4)	=1-F4		
5		=F4	=1-B5			=B4*D4/(B4*D4+C4*E4)	=1-F5		

Next, the row below the hypotheses must be used for labels (column names). Column A must be formatted to acquire the date of the post. Columns B to G must be formatted to acquire probabilities, that is numbers with two decimals. The last two columns, H and I, can be formatted as text, to input the information and its source. In fact, different sources could be used.

Cell B4 is left blank for the analysts to input their prior estimate. Since $P(H_1)=1-P(H_0)$, cell C4 contains "=1-B4". D4 and E4 are left blank for the analysts to input their subjective assessments of the two likelihoods. In cell F4, the following expression has to be inserted: "=B4*D4/(B4*D4+C4*E4)", which is the rule of Bayes. Since $P(H_1|E)=1-P(H_0|E)$, G4 is "=1-F4", so that the probabilities of both hypotheses are displayed explicitly.

The rule of Bayes can be used recursively. In the next row, the posterior of the previous row becomes the prior, therefore B5 is "=F4". Then, all cells containing a mathematical expression are dragged down to copy equations automatically in the lower rows.

Social media analysis

Twitter (www.twitter.com) is a very popular social media - commonly adopted by many politicians - and it is a primary open source of intelligence.

A small set of "tweets" from US President Donald Trump can be used as an example for an early warning task. The acquired information concerns the relationships between the US and North Korea, and must be evaluated in order to quantitatively estimate the risk of an imminent war between the two countries.

After briefly discussing the possibility of a war, analysts input their prior estimates independently. Then, they are given a piece of evidence (a tweet) at a time, allowing them enough time to evaluate it and input its likelihood in case of no war and in case of imminent war. Each time, the posterior probabilities associated to both hypotheses are recalculated automatically and used as a starting point for the following evaluation.

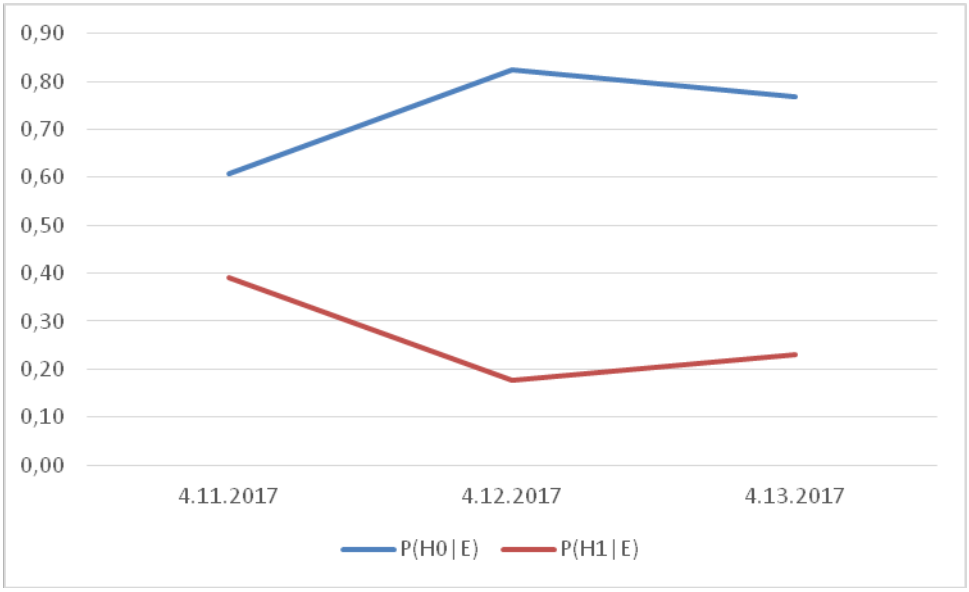
The likelihoods of a piece of evidence do not need to be the complement of each other for the two competing hypotheses. Analysts are free to subjectively evaluate the diagnostic weight of a tweet, which could be even null in case the likelihood of observing it is the same in both cases. For example, the likelihood of a comment by the President on hurricane Irma may be the same (10% or 90%, it does not matter) in case of war and in case of no war. Such information can be deleted, because it is not relevant for the problem at hand. Instead, if $P(E|H_0) \neq P(E|H_1)$, then the information is relevant, and the posterior probabilities associated to the two hypotheses change accordingly.

Figure 2 shows the possible evaluations of three tweets. A linear chart showing the trend of both alternative hypotheses can be added (Figure 3). Line colours must be chosen wisely, in order to ease the readability of the chart.

Figure 2. Estimates.

Date	$P(H_0)$	$P(H_1)$	$P(E\|H_0)$	$P(E\|H_1)$	$P(H_0\|E)$	$P(H_1\|E)$	source	Evidence
11/04/2017	0,70	0,30	0,40	0,60	0,61	0,39	Donald J. Trump @realDonaldTrump	I explained to the President of China that a trade deal with the U.S. will be far better for them if they solve the North Korean problem!
12/04/2017	0,61	0,39	0,60	0,20	0,82	0,18	Donald J. Trump @realDonaldTrump	Had a very good call last night with the President of China concerning the menace of North Korea.
13/04/2017	0,82	0,18	0,50	0,70	0,77	0,23	Donald J. Trump @realDonaldTrump	I have great confidence that China will properly deal with North Korea. If they are unable to do so, the U.S., with its allies, will!

Figure 3. The trend chart.



Discussion and conclusions

Without an electronic spreadsheet and without a good knowledge of statistics and Bayesian inference, it is not easy to calculate the conditional probability of an event given some evidence, even after its likelihood or diagnostic importance has been accurately evaluated by experienced analysts. Two well-known cognitive biases may interfere with the analysts' work: (i) *insufficient adjustment* or *anchoring*, and (ii) the *base-rate fallacy*. In the first case, analysts tend to stick to their first bet $P(H_0)$, regardless of the incoming information (Epley and Gilovich 2006). In the second, analysts evaluate the risk of an event neglecting its prior probability, possibly because of lack of statistical expertise and subsequent adoption of some heuristics (Tversky and Kahneman 1974).

The adoption of Excel can diminish the impact of these biases. If properly formatted and programmed, it can help intelligence professionals to revise their starting hypotheses coherently on the basis of their assessments. Furthermore, thanks to the chart, Excel can help government agencies to track how their analysts' opinions evolve as additional information is collected and evaluated. Thus, managers can easily assess the work of their staff.

Nonetheless, a few issues remain. In particular, analysts may not be able to assess the temporal validity of the collected evidence, even giving for granted that the information is reliable and accurate. Usually, it is not possible to determine whether a piece of evidence is still up-to-date at the time of the final assessment, or even when the following item of intelligence is being evaluated. This problem is closely related to the statement of the alternative hypothesis, that of an "imminent" war. Since it would be useless to evaluate the possibility of a war in the long run, analysts should agree on the meaning of "imminent".

Also the meaning of "war" must be agreed upon. In fact, different definitions may apply. Is a formal war declaration needed for a conflict to be considered as such? Is a single episode where weapons are employed sufficient to declare a state of war? Is it necessary that the attacked part retaliates or not? Is it a war or a terrorist attack if no military targets are hit?

In conclusion, Excel can be a powerful and user-friendly tool for the prediction of a global risk. In particular, it can diminish the weight of biases and ambiguities, assist analysts to state quantitatively their estimates and help decision makers to understand and monitor the situation under scrutiny. However, the *weltanschauung* of the analysts regarding time and war will unavoidably affect any assessment.

References:

1. Barbieri D, (2013), *Bayesian Intelligence Analysis*, in Proceedings of the 19th Conference on Intelligence in the Knowledge Society, Bucharest (Romania), 18th October.

2. Barbieri D, Pressman E, (2015), *Violent Extremists Risk Assessment: A Bayesian Framework*, in Proceedings of the 21st Conference on Intelligence in the Knowledge Society, Bucharest (Romania), 16th October.

3. Bayes T, Price, (1763), *An Essay towards solving a Problem in the Doctrine of Chances*, Philosophical Transactions of the Royal Society, London, no. 53(0), pp. 370–418.

4. Epley N, Gilovich T., (2006), *The anchoring-and-adjustment heuristic: why the adjustments are insufficient*. Psychol Science, April, no. 17(4), pp. 311-318.

5. Fisk C, (1972), *The Sino-Soviet border dispute: A comparison of the conventional and Bayesian methods for intelligence warning*, Studies in Intelligence, no. 16(2), pp. 53-62.

6. Gigerenzer G, Hoffrage U, (1995), *How to Improve Bayesian Reasoning Without Instruction: Frequency Formats*, Psychological Review, no. 102(4), pp. 684–704.

7. Hoffrage U., Gigerenzer G., (1998), *Using natural frequencies to improve diagnostic inferences*. Acad Med., May, no. 73(5), pp. 538-40.

8. Kardes E., Hall R., (2005), *Survey of Literature on Strategic Decision Making in the Presence of Adversaries*, National Centre for Risk and Economic Analysis of Terrorism Events, University of Southern California, Los Angeles, CA (USA).

9. Schweitzer N., (1976), *Bayesian Analysis for Intelligence: Some Focus on the Middle East*. Studies in Intelligence, no. 20(2), pp. 31-44.

10. Sedlmeier P., Gigerenzer G., (2001), *Teaching Bayesian reasoning in less than two hours*. J Exp Psychol Gen., September, no. 130(3), pp. 380-400.

11. Tversky A., Kahneman D., (1974), *Judgment under Uncertainty: Heuristics and Biases*, *Science* New Series, Vol. 185, no. 4157, September 27, pp. 1124-1131.

12. Wheaton K.J., Lee J., Deshmukh H., (2009), *Teaching Bayesian Statistics to Intelligence Analysts: Lessons Learned, Journal of Strategic Security*, Number 1, Volume 2, no. 1: February.

13. Zlotnick J., (1970), *Bayes Theorem for Intelligence Analysis, in Proceedings of the Conference on the Diagnostic Process*, Ann Arbor, Michigan (USA), 18 June.

MONITORING AND ENHANCEMENT OF NEURO-VISUAL PERFORMANCE FOR AIRPORT SECURITY SCREENING PERSONNEL

Cosmin DUGAN[*]

Daniel DINU[**]

Cristian BARNA[***]

Abstract

The aim of the study is to develop a proof of concept experiment dedicated to the monitorization and augmentation of neuro-visual performances in airport security screening personnel. The main specific parameters of the visual tasks involved are visual stereotypy, detection of complex visual patterns, visual-spatial perspective, low-frequency anomaly detection, limited time exposure and psychological pressure. The final result of the research is the development and validation of a neuro-augmentation program.

The rapid development of this branch in the United States (military and civilian spin-offs), the previous interest of some NATO states and similar Romanian civilian initiatives determin~~ed~~ us to propose the foundation of a Human Performance Optimization (or Enhancement) Centre for National Security Personnel. We consider that are at least three main areas of research and development – physical fitness, neuro-augmentation and human-computer interaction.

Keywords: *airport pre-flight security screening personnel, visual task, neuro-visual performances, neuro-augmentation program, low-frequency anomaly detection.*

Introduction

The development of neuroscience and the research aimed at investigating the nervous system and the human mind had a number of outcomes, including military applications. One application is cognitive enhancement or neuro-augmentation, whose goal is to provide to the soldier

[*] PhD student, "Mihai Viteazul" National Intelligence Academy, Bucharest, Romania, dugcosmin@yahoo.com

[**] PhD student, Academy of Economic Studies, Bucharest, Romania

[***] Professor, "Mihai Viteazul" National Intelligence Academy, Bucharest, Romania

cognitive performance, endurance and higher adaptive capacity, while minimizing unwanted effects.

Although there are a significant number of researches and studies on neuro-augmentation and the concern for improving cognitive abilities started since ancient times, this domain is not yet regulated, the terminology is ambiguous and does not enjoy full consensus. The media focus on this subject, in most cases positive and highly optimistic, further contribute to the trivialization and confusion, ignoring the fact that the methods used to improve cognitive performance are largely experimental, and sometimes are risky or invasive.

Terminology and ethical issues

The most important aspect is that, at least for the time being, neuro-augmentation is not a medical procedure in itself. Notwithstanding, it often employs methods that are used for therapeutic purposes within several medical specialties, it is sometimes carried out under guidance by medical personnel and it makes use of data that have been obtained during medical studies or research. The concept appeals to neurological and psychiatric healthy persons and it aims to enable the reaching of an individual's full potential. In doing so, it elevates (cognitive and emotional) individual neuro-psychological performances, on both the quantitative and qualitative levels (the latter implying self-control and personal skills). The approach is similar to the one encountered in sports medicine in the case of high performance athletes.

Other examples are the military (Special Forces, para-troopers, supersonic pilots, astronauts, drivers) and extreme sportsmen (mountain climbers, arctic explorers, deep divers, speleologists etc.). What all these examples have in common is the employment of medical knowledge in order to reach the maximum biological threshold while observing safety precautions and with the full consent and cooperation of the individual, thus making it possible to set personal or collective records.

Neuro-augmentation comprises a soft and non-invasive optimization phase, on the one hand, which is fulfilled through personalized trainings and manipulation of environmental factors as well as an augmentation phase, on the other hand, which may involve invasive and potentially risky methods that might be referred to as doping.

A controversial aspect of the neuro-augmentation concept is dealing with ethical issues that arise from the potential high-scale or highly effective

application of the procedure. The idea of neuro-augmentation itself leads to controversy when questioning the reasons of its potential developers and users, the public opinion and perception, as well as its methods and consequences. Debates on the subject have covered various topics which highlighted a series of challenges following rapid development of research into improving human performance and convergence of strategic and top technologies (such as bio, nano and artificial intelligence).

A first point of interest deals with the types of national or international institutions which will regulate and influence the technologies that are aimed at improving human performance. Equally important are concerns regarding the legal approaches and the political control that will be responsible for the design of such evolutions (Sauter and Gerlinger, 2013, p. 265).

By contrast to other similar practices (e.g. doping in sport), neuro-augmentation is not recognized and regulated by an international treaty. As a result, some voices in the research field are claiming that all courses of action in relation to neuro-augmentation (which range from a *laissez-faire* approach to having it encouraged, enforced as obligatory, allowed or banned altogether) are potentially relevant.

As such, publishing of articles on the subject in top scientific journals is correspondingly challenging, due to the ambivalent status and a lack of a general consensus on the research topic as well as to the absence of specialized institutional authorities in the field. At present, the majority of authors believe that regulations should be issued by state authorities but also incorporated into international guidelines due to their potential social, medical and security implications.

A third point of interest is the context in which neuro-augmentation technologies are used. On the one hand, some authors are advocating for cognitive augmentation as a necessary and mandatory process in connection to claims that there is a direct correlation between an increased IQ and a step-up in productivity. Moral augmentation that might be targeting lawyers, priests or decision-makers at large has its share of staunch supporters as well. On the other hand, some authors urge that all these forms of amplification be categorized as doping and banned altogether. Nevertheless, it is obvious that contextualization of neuro-augmentation practices can produce various interpretations which are not in the smallest degree also influenced by judicial practices or cultural traditions at national level (Dubljević, 2015).

A last point of interest is that lawmakers cannot overlook the fact that the attitude of public opinion is quickly shifting between a highly enthusiastic embrace of the concept, especially in techno-progressive

environments (such as communities of youngsters in cities, Silicon Valley, university town, corporations etc.) (Goertzel, 2015) residing at the forefront of the knowledge-based liberal society and a clear-cut rejection by traditionalists and conservatives.

Further arguments for developing and employing neuro-augmentation techniques are appealing to concepts such as virtue, liberty, cognitive autonomy, utilitarianism, and gaining of new and superior capabilities, which are fundamental topics to consider if neuro-augmentation is to be used ethically (Hughes, 2014).

Within this context the use of neuro-augmentation is justifiable from both the point of view of the utilitarian moral theory, according to which any given action is moral as long as its outcome is positive for as many people as possible and no other damage has been produced, and the point of view of the autonomy principle, which although may be viewed as a personal right stemming from individual liberty, may also be condemned for reasons having to do with social injustice, hedonism, security concerns, and unforeseen consequences.

Risks

In the context of a lack of regulation, the risks ensued by research in the neuro-augmentation field are far from being well defined and mapped. To this purpose, a prospective endeavour in this sense is absolutely necessary.

A primary aspect is constituted by the risk of proliferation of double-use technologies, since neuro-augmentation already employs or will make use of a series of top technologies that have the potential to be exploited for both military and civil purposes. Examples of such technologies are some components of artificial intelligence, neuro-biometrics, brain-computer interfaces, advanced robotics, nanotechnologies, and genetic engineering. Even though these technologies by themselves are strictly controlled and regulated, their convergence can result in products with potential military applications.

The approach is quite similar to the one pertaining to autonomous artificial intelligence. It too is believed to be a double-use technology that may generate major security risks that are difficult to foresee. The pre-emptive argument, which is so abundantly invoked in relation to the emergent technologies in the last half of the century, claims that although the current development state of neuro-augmentation is not posing a serious threat, the next generations stemming from this type of technology will generate major

security risks which are difficult to anticipate and counteract. In light of this argument, super-regulation or banning of military research would have to become a priority.

By invoking similarities with artificial intelligence, another concern becomes apparent. That is the fact that neuroaugmented individuals will become increasingly interested in perfecting the very methods that they have benefited from, as well as dispose of the necessary cognitive resources and other means to learn by themselves at a much faster pace than the rest of the non-augmented individuals. At least in theory, the fusion between human and artificial intelligence by means of neurotechnologies is possible. However, the result would not guarantee predictability in terms of its final utilization and adherence to morality, especially within the military field.

A characteristic of future conflicts will be the employment of Enhanced Human Operations, which are based on the use of man-machine dyads, such as advanced robotics, exoskeletons, directed-energy weapons (neuro) augmented soldiers. Some are fearful that certain countries, which benefit from a lack of legal regulation, the support of the authoritarian political factor, and testing ground in proxy conflicts, are already involved in the development of military augmenting means that can yield an asymmetric advantage.

Research

One of the most important superior cognitive function essential for civilian and military professions relevant for national security is the neuro-visual performance. This was one of the main reasons that motivated our research, alongside the fact that the neuro-visual cortex is well studied and understood. Our research targeted the neuro-visual performances specific to tasks meet in several security related professions: airport pre-flight security screening officers, port facility screening officers, radar operators, image analyst, cyber security officer, UAV pilots, etc. Our research targeted he visual tasks in the case of the airport pre-flight security screening officers. The main specific parameters of the visual tasks involved are visual stereotypy, detection of complex visual patterns, visual-spatial perspective, low-frequency anomaly detection, limited time exposure, psychological pressure.

Our research was aimed at identifying a non-invasive, easy-to-use and safe-to-use method that improves the neuro-visual performance in a short amount of time (3-6 months). Our study was designed as a proof of concept

experiment dedicated to the monitorization and augmentation of neuro-visual performances in airport security screening officers. The final result is the development and validation of a neuro-augmentation program.

The study was carried out on the course of three months, after several preliminary trials dedicated to the improvement of the research methods. We used two groups (study and control, 10 subjects in each group), males and females, smokers and non-smokers, ages between 25-38 years old. The subjects from the first group were informed about the nature of the procedure and signed a consent form. On the course of the three months they were subjected to three different interventions: EEG-neurofeedback, mild pharmacological stimulation and visual training. The EEG-neurofeedback was performed by a specialized neurologist for three months (1 session/week) and the evaluation was made via LORETA analysis[1], using the Neuroguide[2] protocol (functional connectivity analysis).

This is a process that requires experience and successive error attenuation over multiple sessions in order to eliminate the background noise, biases, and insignificant electrical signals. The pharmacological stimulation targeted the cholinergic and GABA-ergic central systems and was also administered for three months. A non-specific neuro-stimulant was also added for 10 days/month. The candidates were monitored weeks and had been instructed regarding safety issues. The tolerance was good, but even if none of the candidates experienced side effects, the subjective experience ("feelings of enhancement") was different. The efficiency evaluation was realised using visual-spatial intelligence tests monitored with eye tracking and EEG recording devices.

Visual training was administered via a commercial app that is available in smartphones and computers (laptop, tablet), for 15-30 minutes/ day (3 days/we). The evaluation in this case was realised using visual intelligence and discrimination task monitored with eye tracking.

The final evaluation consisted in the visualization of specific and standardized Rx images for 8 seconds each (100 images), was administered at the beginning and at the end of the study. We tried to replicate most of the real-life conditions (noise, illumination, irregular distractions, random blank images interposed). The neuro-visual performance was evaluated using

---

[1] LORETA is the acronym for standardized low resolution brain electromagnetic tomography, method used for localizing the electrical activity in the brain based on scalp potentials from multiple-channel EEG recording

[2] https://bio-medical.com/neuroguide-deluxe-qeeg-255.html

electroencephalography (EmotivEpoch – 14 channels EEG and MindWawe Mobile - single channel), visual interaction (Tobi eye-tracking device and CoolTool platform) and galvanic skin response (a channel). The raw data obtained was processed using several specific software and the results interpreted and compared with similar studies.

Results

The fusion and interpretation of the information obtained from different channels was a complex task, with some of the issues still necessitating further optimization. For example, we persistently observed a high variability in the electroencephalographic recording that attenuated in most of the cases after 10 or more minutes after the beginning of the work sessions (near-real occupational exposure). Major differences were also observed in the electric activation patterns between males and females and smokers and non-smokers (nicotinic receptor activation?).

Using LORETA analysis (EEG, 14 channels, minimum of 20 minutes of evaluation) we observed a stable and robust frontal and occipital activation in all of the cases. Alpha wave asymmetry in the frontal lobes after visualization of "high value targets" was also identified and observed consistently even in non-expert subjects.

An even higher variability was observed in galvanic skin response (GSR) recordings, even on the same person on different sessions. A number of factors, such as clothing, electrostatic loading, emotional status etc. (unrelated to the study) have a major contribution to the variations in the GSR signal. However, by making multiple recordings and integrating the GSR recordings with the rest of the data obtained emotional polarity, emotional intensity variations or stress effects can be observed and measured.

On contrary, multiple sessions of eye-tracking led us to the conclusion that the visual search patterns (visual strategies) are relatively constant in an individual, and can be used for biometric recognition. The improvement of the visual search performance as a result of visual training and adherence to the study was best monitored using (first generation) eye tracking. In the context of the accelerated development of the brain-computer interfaces based on visual interaction, we consider eye tracking is a non-invasive method, easy to use and with a large potential.

The small number of subjects and the fact that our study was concept proof limited our possibilities of expressing the results in a statistical manner, but allowed comparative assessments or case studies to be carried out. The comparative assessments performed on the same subject (individual assessment) showed that the range of the improvement before and after the successful completion of all three interventions varied between 30% -100%.

Performance improvement in (presented as an average of end-of-run performance) between the control and the augmented lot was about 50%, but this assessment should be seen as a partial quantitative indicator. The most important indicators, with predictive capacity, were those used to evaluate the visual search strategies. In the case of electroencephalography there was an increased interpersonal variability which limited the possibility of being used in intergroup comparative evaluations.

The results obtained so far are positive and show a remarkable improvement in pattern detection, the speed of anomaly detection, a decrease in false-positive target detection, optimized visual search patterns, improvement of signal/noise ratio and general visual efficiency improvement.

Conclusions

The majority of authors acknowledges the necessity of a regulation framework for certain aspects of neuro-augmentation and connected emerging technologies. This is all the more true when considering the modern-day global race for increased social, economic, political and military competitiveness. For organizations dealing with national security, efficient management of resources is a crucial objective that needs to be met as a result of the current dynamics of the security environment. As such, any investments in neuro-augmentation technology needs to be balanced by its benefits and the extent of risk control arrangements.

Talking about the outcome of our study we consider that the research showed that the limits for human performance improvement and in particular for higher cognitive functions are not exhausted. Today's expanding technological environment is the main driver for human performance improvement development. Security risks and threats, and in particular terrorism and the proliferation of non-state hostile intelligence services, forced changes of strategy and human element improvement convergent with internet and artificial intelligence development.

Our proof-of-concept research highlighted the potential of neuro-augmentation methods and the possibilities for use in national security professions. Neuro-visual improvement can be useful in several professions of interest for national security and represent a complementary niche for research on computer vision and artificial intelligence.

Our final statement is that EEG-neurofeedback, mild pharmacological stimulation and visual training (together with other methods) can be useful in training and efficiency improvement for pre-flight airport x-ray security screening personnel.

References:

1. Beyer, Chad, Staunton, Ciara, Keymanthri Moodley, (2014), *The implications of Methylphenidate use by healthy medical students and doctors in South Africa*. BMC Med Ethics, available at http://bmcmedethics.biomedcentral.com/articles/10.1186/1472-6939-15-20.

2. Dingwall, Robert, (2008), *Shaping the Future of Humankind: Three Commentaries on The Ethics of Enhancement*. Health Economics, Policy and Law.

3. Dubljević, Veljko, (2015), *Cognitive Enhancement: Ethical Considerations and a Look into the Future*. in Shira Knafo, César Venero. *Cognitive Enhancement*. Elsevier.

4. Goertzel, Ben, (2015), *Technoprogressive Political Platform for the USA*, available at http://ieet.org/ index.php/IEET/more/goertzel20151107.

5. Heinz A., Kipke R. (2012), *Cognitive neuroenhancement: false assumptions in the ethical debate.* J Med Ethics, vol. 38, available at http://www.ncbi.nlm.nih.gov/pubmed/22228818.

6. Hughes, J., (2014), *Ethical Arguments for the Use of Cognitive Enhancing Drugs (Part Two)*, available at http://ieet.org/index.php/IEET/more/hughes20140314.

7. Ignatius, David, (2016), *The exotic new weapons the Pentagon wants to deter Russia and China*, February 23, "The Washington Post", available at https://www.washingtonpost.com/opinions/the-exotic-new-weapons-the-pentagon-wants-to-deter-russia-and-china/.

8. Sauter, Arnold, Gerlinger. Katrin, (2013), *The Pharmacologically Improved Human Performance-Enhancing Substances as a Social Challenge*. Final Report, Technology Assessment Studies Series, No 5, 2013, available at http://www.itas.kit.edu/pub/v/2013/sage13a.pdf.

AN ANALYSIS OF PRIVACY AND ANONYMITY IN THE CRYPTOCURRENCY FIELD

Cristina CARATA (GURĂU)[*]

Motto:

"The one thing that's missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A. The way I can take a $20 bill hand it over to you and then there's no record of where it came from. You may get that without knowing who I am. That kind of thing will develop on the Internet and that will make it even easier for people using the Internet. Of course, it has its negative side.

It means the gangsters, the people who are engaged in illegal transactions, will also have an easier way to carry on their business." (Milton Friedman, 1999)[1]

Abstract

In the society we live in today, financial confidentiality and privacy has become an important topic on the agenda, due to the fact that it is a concept embracing both data security and private life data security. Crypto-currency has brought forth new concepts, some of them even innovative - unknown to this date in the currency field - that can fundamentally change the way we look at payment systems.

Virtual coins are based on cryptographic protocols and proof-of-work protocols (based on hashing algorithms) as security methods. Thereby, "digital wallets" and digital currency transactions are safe, irreversible and do not contain personal information from the user. In addition to this feature, virtual money payments can be made without personal information being linked to the transaction. Thus, since the emergence of the first virtual coin – bitcoin, in 2008 - cryptocurrencies quickly developed as a popular digital payment system, largely due to these fundamental features.

The present paper is intended to analyse why cryptocurrencies are becoming more and more popular due to the notions of "privacy" and "anonymity", the innovative technology used and the effects of such anonymous transactions: on one hand, the protection of personal data and fluency of financial transactions and, on the other hand, the use of this technology in illegal activities.

Keywords: *cryptocurrency; privacy; anonymity; technology; data security.*

---

[*] PhD student at „Mihai Viteazul" National Intelligence Academy, Bucharest, cristina.carata@yahoo.com

[1] Milton Friedman (July 31, 1912 – November 16, 2006) was an American economist who received the 1976 Nobel Memorial Prize in Economic Sciences for his research on consumption analysis, monetary history and theory, and the complexity of stabilization policy.

Introduction

The first monetary system known in history appeared in Mesopotamia, around 3000 BC, when the inhabitants of those territories began to use silver as a medium of exchange and as a unit of value. The moment coincided with the emergence of Hamurabi's code-a code that contained a set of rules for monetary exchanges through silver. Since then, the monetary system has experienced drastic and constant changes, including paradigm shifts.

Without aiming to analyse the changes the monetary system has gone through since its emergence until present days, of interest for the present article, in today's society, are the modern banking services, especially online banking. Remote Banking services through electronic means (shortly e-banking system) began to develop since 1995, the year in which the US Presidential Bank of Mariland launched its first online banking services (through internet). E-banking services use computer and electronic technologies as a support for payments and other document transfers. Because of the rapid changes in the IT domain, banks face specific risks regarding electronic banking and electronic money, especially in terms of customer data security (Georgescu-Goloşoiu, 2006).

As we speak, one of the issues that is appearing more and more often is the one of financial confidentiality and privacy, in the light of cyber threats increasingly more present in our everyday life. This topic has become an important one on the agenda, due to the fact that it is a concept embracing both data security and private life data security.

Over the past few years, data breaches have increased in frequency and size, making the need to protect sensitive information a top priority for businesses worldwide. According to a 2015 report, there have been more than a thousand worldwide data breaches that compromised nearly 563 million data records of customers' personal and financial information. Big names targeted and exposed in the last 12 months not only include Ebay, Adobe, Tesco and Morrisons, but also reputable financial institutions such as the European Central Bank, JP Morgan Chase and HSBC (*Hampton, 2015*).

Given that in recent years, especially because of the exponential technological progress, companies – including here banks as part of the monetary system - are gathering an increasingly bigger number of consumer data, more and more of them are concerned about maintaining confidentiality, in terms of their personal behaviours and information. Studies conducted mainly following the events of September 11, 2001 in the United States of America – a moment that marked an increase in the control of personal data, on a global scale, in order to combat the growing phenomenon of terrorism - show that people are more concerned about the security of their personal data

and are more aware of the fact that more and more data is being collected. The vast majority of people consider that they have lost control over their personal data, which has generated considerable concern. The biggest crackdown is the fact that companies - by default, banks - which collect all this information and personal data will not be able to store them safely.

An increasingly common problem is the trade-off between security needs and personal privacy. In other words, the question that emerges is at what point security will undermine the open society that we are trying to protect and how much personal freedom should we give up to be safe, both we and our data?

In the light of these growing concerns over the last two decades, one of the most important services that the banking system can do is to ensure the privacy of its client's data and personal information. Assuring data protection in the age of the Internet can be a relatively complicated issue, especially with regard to online transactions, but without forgetting the basic issues of pure personal data previously presented.

Because of all these concerns - on one hand, cyber-attacks that are more common in the online banking system and the threat regarding both personal data and patrimonial assets held in accounts and, on the other hand, personal intrusion - a growing number of people are turning their attention towards alternative financial solutions, one of which is the use of digital coins or *crypto-currencies*, such as *bitcoin* (the first and most popular currency of its kind, a benchmark in the field)

Why are *crypto-currencies* an alternative to the classic banking system?

Crypto-currencies are gaining more ground, in parallel with the decline of the public confidence in the classical banking system and other traditional financial institutions and as a response to personal data security issues. At the same time, *crypto-currency* has brought forth new concepts, some of which are even innovative - unknown to this date in the currency field - that can fundamentally change the way we look at payment systems. In technical terms, *crypto-currency* or virtual currency is a non-banking and decentralized method (supported by its users) to exchange value between individuals, peer-to-peer (bidirectional, without intermediary) and based on cryptographic protocols and proof-of-work protocols (based on hashing algorithms) as securing methods (Carata, 2017, pp. 192-198).

Since the emergence of the first digital coin in 2008 - *bitcoin*, which has remained the most popular virtual currency so far - the scale of the phenomenon

led to the appearance, as we speak, of over 700 types of digital coins, or *crypto-currencies*, called altcoins. And the prospects for increasing the number of virtual coins are developing due to their popularity and media coverage.

The features of *bitcoin* - and at the same time, the features of the large majority of *crypto-currencies* - are strong arguments for their users regarding the decision to use them at the expense of classical banking systems. "Firstly, *crypto-coins* do not exist in physical form (they are digital coins without a classical representation in physical form) and, most importantly, they are a decentralized payment form. So, they are not created or controlled by any governmental institution, nor regulated. Secondly, virtual coins are based on cryptographic protocols and proof-of-work protocols (based on hashing algorithms) as security methods. Thereby, digital currency transactions are safe, irreversible and do not contain personal information from the user. In addition to this feature, virtual money payments can be made without personal information being linked to the transaction - or, at least, apparently, as we'll see below. Thirdly, international virtual money transfers have features that are not applicable to classical payment systems: they are almost instantaneous, there are no commissions in the classical sense of the term for the transfer of the virtual currency, there are no "third parties" involved- which eliminates the so-called "danger" of others having access to sensitive personal data, the transfer is peer-to-peer, without intermediaries and there is no maximum transfer limit or a limit over which transfers are controlled or examined by various institutions (Carata, 2017, pp. 192-198).

Due to this characteristics, for many of its users, *crypto-currency* can provide greater security, privacy, anonymity and flexibility compared to the conventional centralized financial system and, as a result, a much better way to conduct financial transactions while protecting their personal data.

A short analysis of privacy and anonymity in the *crypto-currency* field

One of the most controversial aspects regarding *crypto-currencies* is security, privacy and anonymity. The three notions, albeit similar, are not identical, especially with regard to the online domain. In short, privacy is the control over one's personal information or actions, security represents the freedom from risk or danger, and anonymity can be defined as being unidentifiable in one's actions (Romanosky, 2011).

First of all, *crypto-currencies* are a decentralized payment form and are not created or controlled by any governmental institution, nor regulated, as we speak. To put it in simple terms, instead of a government that prints money for economical purposes via central banks, in the *crypto-currency*

system, every user can "create" its money by *mining* (the mining process implies that users use a specific mining program that solves different algorithms in order to release blocks of coins into the network-in circulation). Furthermore, instead of putting trust in governments and the banking systems to back a currency and maintain its value, the value of the *crypto-currencies* comes from the network of people using it. As a result of all this, no private data are exposed to third parties in transactions – in the classical banking transactions, the third parties are represented by banks, that have access to all the information regarding it and the users involved.

As we have seen before, *bitcoin* – and largely all *crypto-currencies* – are based on a "peer-to-peer (P2P) architecture, which means *crypto-currency* users are able to issue transactions carrying payments in *bitcoins*. To provide some form of anonymity, direct personally identifiable information are omitted from any transaction; instead, source and destination are encoded in the form of public keys, which serve as pseudonyms. Every party can generate as many public keys as he wishes; the corresponding private keys are used to authenticate (sign) transactions and are stored in private wallets either locally on a user's computer or in cloud-storage providers (Ober, Katzenbeisser and Hamacher, 2013).

Furthermore, the block chain technology used by the virtual coins requires that the transactions be exposed in a public register. So, due to the fact that all transactions are stored publicly in the block chain, the anonymity of a user relies on the pseudonym not being linked to his true identity (Möser, 2013).

So, at a first glance, *bitcoin,* as well as all the others *crypto-currency*, is not really anonymous but just hides the true identity of the users behind some pseudonyms. For example, user A transfers to user B a sum of 10 *bitcoins.* Even though the identities of the two are not known, the transaction is still public, for an infinite term.

Last but not least, an aspect of particular interest in terms of "privacy" and "anonymity" in the *crypto-currency* is that related to the transfers of such digital coins. Thus, virtual currency transfers have a feature that is not applicable to classical banking systems: there is no maximum transfer limit or over which transfers are verified by different institutions. In simple words, regardless of the amount transferred between different users or the amounts withdrawn from user accounts, no additional personal data is required. Once transferred, electronic coins can be exchanged in the "classical" currency, such as the euro or dollar, anywhere in the world, through *crypto-currency* "exchanges". No additional verification or validation should be necessary to execute any transaction.

As a first conclusion, based on the arguments previously exposed, *bitcoin* - and the vast majority of digital coins - is built to allow its users to send and receive payments without exposing as much personal data as with classical money transfers and with increased security against hacker threats. However, *bitcoin* – as well as other *crypto-currencies* - cannot be considered anonymous. They only ensure a much higher level of privacy regarding personal data than the classic banking system. As we have seen before, the use of bitcoin leaves traces in the public ledger: all transactions are indefinitely public, even if the real identity of the users is unknown.

A special case in the privacy and anonymity domain of *crypto-currencies*, compared to the features outlined above, is represented by *Zcash* and *Monero* coins.

Due to the fact that *bitcoin* and altcoins in general are not really "anonymous" virtual coins but only offer a higher degree of privacy compared to the classical banking transactions and due to the fact that the need for anonymity remains a topic of high interest among users of this type of coins, *Zcash* appeared on the market.

Zcash is another *crypto-currency* like *bitcoin*, created in 2016 (based on an earlier 2014 protocol) through a collaboration between the researchers at Johns Hopkins University and a group of cryptographers at the Massachusetts Institute of Technology, the Technion – Israel Institute of Technology and Tel Aviv University. Although structurally similar to *bitcoin* and other altcoins, *Zcash* uses innovative cryptography techniques that allow increased privacy and anonymity for its users. In the case of *Bitcoin* and the so-called "traditional" *crypto-currencies*, a transaction consists of an origin address, destination address and the amount transferred. All these transactions are available on a decentralized ledger: the block chain. Because the block chain is public, the history of all transactions can be viewed by anyone. While addresses are not explicitly tied to users' real identities, recent studies have shown that the block chain can be mined to learn information about users' spending habits. *Zcash* extends *Bitcoin*'s protocol by adding new types of transactions that provide a separate privacy-preserving currency, in which transactions reveal neither the payment's origin, destination, or amount (ZeroCash Official Website).

In addition, according to its developers: "*Zcas*h enhances privacy for users by encrypting sender, amount and recipient data within single-signature transactions published to its public block chain ledger". Also "*Zcash* has a distinct advantage in terms of transaction privacy and as a result, anonymity" (ZeroCash Official Website).

So, at a first glance, *Zcash* takes the cryptographic technology of *crypto-currencies* at an innovative level that allows truly anonymous transactions between its users.

In the other case, of *Monero* virtual coin, its creators are unknown to this date (the only available information is a pseudonym of "thankful_for_today"). Just like *Zcash*, although structurally similar to *bitcoin* and other altcoins, *Monero* uses different innovative technologies to enhance the privacy and anonymity of its users.

Unlike most of the digital coins, *Monero* uses a special technology called "ring signatures" which shuffles users' public keys in order to eliminate the possibility to identify a particular user. Untreaceability doesn't protect a receiver from defining his or her balance through inspecting ingoing messages to the user's public address. Therefore, *Monero* employs a specific protocol which generates multiple unique one-time addresses that can only be linked by the payment receiver and are unfeasible to be revealed through block chain analysis. Like any other digital currency, *Monero* is cryptographically secured. Though, the peculiarity of algorithm consists in tremendous computational and electric capabilities that a hacker would need to try to obtain private information regarding the identity or the transactions.

Enhancing privacy and anonymity: TOR

Undoubtedly, *crypto-currencies* - whether we're talking about *bitcoin* or *Zcash* - have a degree of privacy and, sometimes, even anonymity that determine a growing number of people - worried about the security of their personal data and of financial transactions facing hacking threats – to choose them as an alternative financial instruments to the classic financial system.

An additional argument for choosing these alternative financial instruments is to use them together with other innovative technologies, such as anonymous communication technologies, like Tor, to further enhance data protection.

In the case of any communication and transaction system - including financial ones - the issue is to ensure anonymity and security between the information flowing through the network, between senders and recipients, against unwanted attacks outside the network. One of the technologies that ensure this is Tor - a technology that can be used successfully along with *crypto-currency* transactions.

Tor was originally a project created by the American Navy Research Laboratories to protect the online communications of United States of America governmental organizations. As we speak, it is a software that is used globally by users who value the anonymity of their online activity and is represented

by a non-profit organization whose primary purpose is the research and development of tools that offer privacy online.

From a technical point of view, Tor hides the real identity of the user who accesses different sites or carries out various transactions, "strolling" the information through different Tor servers, encrypting the traffic so that the user cannot be traced. The difference between Tor and conventional internet addresses is that Tor uses encrypted addresses with hidden content. Virtually Tor comes to replace classic browsers used in Internet browsing - like Chrome or Firefox. Any communication conducted through the Tor browser is safe, with the main application of being safe in the face of hacker attacks. The data is grouped in encrypted packets before entering the Tor network. After this moment, Tor removes part of the header of this package, which includes information such as the source, size, destination, and timing, all of which can be used to find out about the sender. Next, Tor encrypts the rest of the information, which a normal internet connection cannot do. Finally, encrypted data is sent through many randomly assigned servers, each of which decodes and then re-encrypts enough data to know just where it came from and where it goes.

Even if the two technologies, Tor and *crypto-currencies*, apparently do not have much in common, yet used together considerably increase the degree of privacy and anonymity in the case of financial transactions conducted through alternative financial instruments. Because almost all *crypto-currency* transactions – except the case of *Zcash and Monero* - are stored on the block chain, the data stored includes an amount transferred and the addresses of the sender and the recipient. So every payment has a traceable history that can be viewed by anyone. However, as we have seen before, these addresses are not themselves linked to a person or entity, however a person's identity can be associated with an address through other means. This is the point where Tor software can help protect identity and data. When a *crypto-currency* transaction is run through Tor, the chances of attacks by hackers on the transaction itself or personal data drop dramatically due to the cryptography of the previously presented data.

Conclusions

Throughout the world, technology has reached almost all domains: we are witnessing a spectacular technological advance that has revolutionized all areas, from medicine, education and the aerospace industry to the financial one. And evolution does not stop here. Although in the vast majority of cases the spread of state-of-the-art technologies in all fields offers visible benefits, as a side-effect, we can also discuss about the emergence of potential threats.

This is also the case for personal data protection and the security of financial transactions that are increasingly targeted by hacker attacks and beyond.

The desire to protect data and to secure security leads an increasing number of people to turn to alternative financial services, such as *crypto-currencies*, which, at least apparently, offer a higher degree of protection than the classic alternatives provided by banks. *Crypto-currencies* have become a reality of our days that can no longer be ignored. More and more institutions are turning their attention to this alternative method of payment. For example, the European Union has begun amending its legislation (Directive 849 of 2005), the Japanese government is taking the first steps for the official recognition of *crypto-currencies* and Norway's largest online-only bank, Skandiabanken, recently announced plans to offer customers the ability to link bank accounts to *crypto-currency* holdings. A clear benefit for *crypto-currency* users is the privacy and personal data security. Problems like internal fraud by bank employees that sell the customer data, spammers or scammers are removed in this way. As we have previously shown, the data of *crypto-currencies* users are harder to track.

But there are also controversies about the use of *crypto-currencies* in illegal activities. A recent example is the "WannaCry" malware attack from mid-May 2017, when data on thousands of computers, both individuals and institutions, were encrypted and the required reward was in *bitcoin*. Undoubtedly, the characteristics of virtual coins to represent a decentralized payment form (therefore not created or controlled by any governmental institution, their issuance is not supervised by any central authority nor regulated), the anonymity of its users and their transactions make it more attractive for those who engage in illegal activities and have begun to raise numerous alarm signals for institutions and countries around the world lately. For example, Thailand was the first state in the world to ban the sale and purchase of bitcoin coins or products using this payment system. The decision was motivated by the fact that there are very few laws and capital controls in this area. Soon, in 2014, Russia also followed, which motivated its decision by the fact that the Russian legislation provides for the rouble as the only official currency and the introduction of any other currency or substitute is strictly forbidden.

The antithesis of using *crypto-currencies* for illegal purposes is their use for charitable purposes. Recent news reveal the fact that The United Nations World Food Programme (WFP) uses the Ethereum Blockchain[2] to transfer vouchers based on *crypto-currencies* to refugees in Syria. Completed

[2] Just like Bitcoin, Ethereum is a descentralized cryptocurrency. According to its official website (www.ethereum.org), Ethereum is a decentralized platform that runs smart contracts

on 31st May, the project run by the WFP was designed to direct resources to thousands of Syrian refugees by giving them *crypto-currency*-based vouchers that could be redeemed in participating markets (De Castillo, 2017).

***

Virtual currencies will ultimately be subject to existing regulations in the financial domain and other supplementary systems (as is the case with EU Directive 849/2005). In addition, virtual coins cannot be more "anonymous" than cash and cannot hinder official authority investigations. Also, the whole *crypto-currency* system is built to prevent a wide range of financial irregularities.

References:

1. Carata (Gurău), Cristina, (2017), „Modern methods of financing terrorism in a global and intercultural society: *crypto-currency", Redefining community in intercultural context*, Vol. 6, No.1, pp. 192-198, accessed 1 September at http://www.afahc.ro/ro/rcic/2017/RCIC'17/rcic'17_volume.PDF.

2. De Castillo, Michael, (2017), *United Nations Sends Aid to 10,000 Syrian Refugees Using Ethereum Blockchain*, June 13, accessed on 11 September 2017 at https://www.coindesk.com/united-nations-sends-aid-to-10000-syrian-refugees-using-ethereum-blockchain/.

3. Georgescu-Goloşoiu, Ligia, (2006), *Electronic Banking/E-Banking, Editura Economică*, Bucureşti, 2006 accessed 7 September 2017 at http://ligiagolosoiu.ro/content/Servicii_bancare_electronice.pdf.

4. *Hampton, Paul, (2015), Why banks need a different approach to data security, January 9, accesed 11 September 2017 at* https://www.globalbankingandfinance.com/why-banks-need-a-different-approach-to-data-security/**.**

5. Möser, Malte, (2013), *Anonymity of Bitcoin Transactions An Analysis of Mixing Services*, Münster Bitcoin Conference (MBC), 17–18 July, Münster, Germany, accessed 2 September 2017 at https://www.wi.uni-muenster.de/sites/wi/files/public/department/itsecurity/mbc13/mbc13-moeser-paper.pdf.

6. Romanosky, Sasha, (2011), *Privacy vs. Security vs. Anonymity*, January 4, accessed 3 September 2017 at https://concurringopinions.com/archives/2011/01/privacy-vs-security-vs-anonymity.html.

7. Ober, Micha, Katzenbeisser, Stefan and Hamacher, Kay, (2013), *Structure and Anonymity of the Bitcoin Transaction Graph*, Future Internet, no. 5, pp. 237-250, accessed 2 September 2017 at http://www.mdpi.com/1999-5903/5/2/237/htm.

8. ZeroCash Official Website, accessed on 8 September 2017 at http://zerocash-project.org/.

INTRODUCING INTELLIGENCE ENGINEERING: OPERATING BEYOND THE CONVENTIONAL

Adam D.M. SVENDSEN *

Abstract

Contemporary defence and security efforts can be viably improved. With an overarching focus on 'ways', 'means', up and across to realising operational and strategic-ranging 'ends', this article advances a substantially-structured, multi-scaler 'intelligence engineering' (IE)-based framework and 'step-by-step' toolbox useful for both deployment and employment for a multitude of purposes - essentially whatever is to be accomplished. As this article goes on to reveal, the IE framework can contribute towards helping progress several intelligence and knowledge-related tasks. Both 'situational awareness' to deeper-ranging 'contextualisation' assistance value is offered. Demonstrating how they can be best harnessed, the different process 'steps' cover diverse areas such as, inter alia: 'focus/topic selection' through to the fashioning of 'signifier node(s)' for helping in decision-making both now and into the future. Concluding, this article highlights that the entire process involved facilitates: (i) greater risk appreciation; and then (ii) subsequent risk management; as well as even advancing (iii) risk engineering to resilience qualities, in overall defence and security enterprises and endeavours during an era when much uncertainty is encountered.

Keywords: *intelligence, intelligence engineering, 'step-by-step' toolbox.*

Introduction

This article introduces and further advances the concept of '*Intelligence Engineering*' (IE).[1] At its most diverse, IE is defined as:

> *the use of scientific and technical knowledge to artfully bring about (deliver or implement) the design, building, and use of engines, machines, and structures, and equally the study and activity related to the modification or development of those*

* PhD (Warwick, UK) is an intelligence & defence strategist, educator, researcher, and consultant, adam@asgonline.co.uk

[1] Due to the constraints of limited space in this short introductory article, for more detailed insights into 'Intelligence Engineering', readers are directed to see as discussed throughout the book, A.D.M. Svendsen, *Intelligence Engineering: Operating Beyond the Conventional* (New York: Rowman & Littlefield / Security & Professional Intelligence Education Series - SPIES, 2017).

> *entities, in order to imagine, design, create, make, operate, maintain, and dismantle complex devices, machines, structures, systems, and processes that support and/or disrupt human endeavour occurring both in and/or overlapping with the more specific intelligence context—spanning both human intelligence (HUMINT) and technical intelligence (TECHINT) realms…*

In turn, the intelligence context:

> *[S]ignificantly involves the collection and processing (analysis) of information that is particularly of military and/or political value, and which especially (and purposefully) relates to international relations, defence, and national (extending to global, via regional) security (threats, encompassing at their most broad, the full-spectrum of issues-problems-hazards-up-to-risks confronted). The last of these efforts frequently also involves secret (covert and/or clandestine), and often (although not exclusively—as private and sub-/non-state actor contributions are also included) state activity conducted by specialized 'intelligence' institutions (or organisations) to understand or influence entities.*[2]

In its main, this article contends that the 'IE framework' that is introduced and advanced here is relevant for several key reasons. Notably, these reasons include such as for the *functional purposes* of: first, conducting successful risk analysis and assessment/estimate work; to, second, for assisting with risk management activities; and for, third, helping to facilitate resilience in overall defence and security-related contexts (however those contexts are precisely conceived in all of their detail).[3]

This article further argues that IE work is done for much-needed sophisticated: (a) 'context appreciation' and deeper-to-wider understanding/ knowledge-related work (namely, recognised analysis and assessment/ estimation - e.g. G/J2 Intelligence - activities); and then (b) improved 'solution-fashioning', relating to event and development shaping and transformation tasks (acknowledged as engineering and building/synthesis - e.g. G/J3 Operations/Training - efforts).[4]

---

[2] *Ibid*, pp.19-20.
[3] *Ibid.*, p.25.
[4] See also A.D.M. Svendsen, 'Advancing "defence-in-depth": Intelligence and systems dynamics', *Defense & Security Analysis*, 31, 1 (2015), pp.58–73, and A.D.M. Svendsen, 'Contemporary intelligence innovation in practice: Enhancing "macro" to "micro" systems thinking via "System of Systems" dynamics', *Defence Studies*, 15, 2 (2015), pp.105–23.

Ultimately, the overarching aim of IE is for, firstly, fostering better understanding, and then, secondly, for addressing *complex uncertainty* - a condition that is experienced both now at present and that is readily anticipated to persist in the future. For example, this is as that uncertainty occurs both in and across the full-spectrum range of various operational- to battlespaces from 'war'-to-'peace', as well as more strategically when it exists in a greater overarching manner.[5]

Throughout the conduct of Intelligence Engineering work, there is a strong focus on what can be best termed as 'positioning' and/or 'posturing'. Adoptions of these stances can be summarised, for instance, as better getting 'ahead of' event and development 'curves' as they unfold temporally, at times rapidly. Both *a priori* (before/ahead) and *post facto* (after/behind) concerns and considerations therefore feature substantially - closely relating to situations, events and developments both encountered and experienced (reactively), and/or perhaps even about to be encountered or experienced through their anticipation (more proactively).[6]

The Intelligence Engineering (Ie) Approach

At its most distilled, Intelligence Engineering offers its practitioners, followers and implementers several tools, toolboxes and toolsets they can readily access for use. This approach is represented, for instance, by the harnessing of increasingly familiar 'System of Systems' or 'Federation of Systems' (SoS) concepts, such as represented by PMESII, which relates to Political, Military, Economic, Social, Informational/Intelligence, and Infrastructural indicators and factors - as already used for some years, for example, in the North Atlantic Treaty Organisation (NATO) and during the course of its analysis/assessment (estimation) work.[7]

---

[5] See, for example, as discussed throughout, *inter alia*, G. Eriksson and U. Pettersson (eds.), *Special Operations from a Small State Perspective: Future Security Challenges* (London: Springer, 2017) and C.G. Kwa, 'Postmodern Intelligence: Strategic Warning and Crisis Management', chapter in F. Baudet, E. Braat, J. van Woensel, A. Wever (eds.), *Perspectives on Military Intelligence from the First World War to Mali: Between Learning and Law* (London: Springer, 2017), pp. 97-118; see also A.D.M. Svendsen, 'Brexit: an agent of "disruptive change" for UK and European intelligence?', *Journal of Intelligence History* (2017).

[6] Svendsen, *Intelligence Engineering*, esp. p.25, p.74 and p.87; see also A.D.M. Svendsen, 'Strategic Futures and Intelligence: The Head and Heart of "Hybrid Defense" Providing Tangible Meaning and Ways Forward', *Small Wars Journal - SWJ* (June 2017).

[7] For more SoS background insights, see via Svendsen, *Intelligence Engineering*, p.144, col.1; for the value of indicator approaches in intelligence analysis contexts, see also L. Madureira, 'Market and Competitor Analysis: Real Exercise', ch. 8 in W.J. Lahneman and R. Arcos (eds), *The Art of Intelligence* (NY: Rowman & Littlefield, 2014), p.133; R.H. Pherson and John Pyrik, *Analyst's Guide to Indicators* (US: Pherson Associates, LLC, 2017).

Perhaps more helpfully, offering advantage, IE also guides its users as to which SoS-based tools, toolboxes and toolsets (such as PMESII introduced above) are the best ones to select and apply. Indeed, this selection or choice consideration resonates whatever the context that might be precisely experienced and encountered (and however, in whichever circumstances), pointing to - at least a degree of - claimed 'multi-scaler' utility that belongs to the overall IE approach (pertaining to its use or help in a number or multitude of differing contexts).[8]

Adopting sheer marketing perspectives, Intelligence Engineering having several tools, toolboxes and toolsets embedded within its overarching approach demonstrates much to several different stakeholders from producers to consumers. What can be communicated most readily here in this article is the 'added value' in the form of 'unique selling points' (USPs) IE overall brings to multiple defence (including military) and security (including policing/law-enforcement) enterprises, such as those ranging across the 'war'-to-'peace' environments, as characterised earlier (see above), and including the high-profile, continuing contemporary fight against so-called Islamic State (IS) - also known as the Islamic State of Iraq and al-Sham or Syria (ISIS), the Islamic State of Iraq and the Levant (ISIL), and Da'esh.[9]

Breaking-Down Intelligence Engineering Into Its Components

To provide a comprehensive summary by way of its further introduction, the IE 'toolbox' consists of five 'toolsets', which each offer a series of 'tools'. Each 'toolset' is also representative of a digestible, 'bite-sized' IE process 'step'.

The different, five Intelligence Engineering process 'steps' drawn upon during the course of pursuing the overall IE approach, cover diverse areas, such as, *inter alia*: (1) 'focus/topic selection' for helping in targeting and with prioritisation tasks; (2) ascertaining which 'federation or system of systems dynamics' are chosen to employ or draw upon during analysis and assessment/estimate work when evaluating entities and/or situations, such as PMESII (see as outlined earlier); (3) the different 'system variables/ attributes' involved, and (4) the 'levels' of experience and hence analysis-to-

---

[8] Svendsen, *Intelligence Engineering*, p.85 and p.104; in a 'hybrid defense' context, see also Svendsen, 'Strategic Futures and Intelligence'.

[9] See, for example, as discussed in A.D.M. Svendsen, 'Developing international intelligence liaison against Islamic State: Approaching "one for all and all for one"?', *International Journal of Intelligence and CounterIntelligence*, 29, 2 (2016); see also 'UK launched cyber-attack on Islamic State', *BBC News* (12 April 2018).

engineering to consider; and (5) the fashioning of 'signifier node(s)' for helping make decisions and for generating 'where next?' responses.[10]

In turn, each IE process 'step' can then be progressed linearly, in sequence, from beginning to end in a highly 'building' and/or 'shaping' or 'framing' manner. Overall, the IE process is arranged as a (semi-)structured analytical framework for risk, offering a lens that provides both intelligence analysis and more advanced Intelligence Engineering inputs to wider processes, extending to the comprehensive evaluation of situations, events and developments, including surrounding their awareness and even steering.[11] Several defence and security endeavours to enterprises gain broadly.

IE Value

As demonstrated thus far, when presented in terms of its 'value', IE clearly boasts many instantly recognisable operational and up and across to strategic 'ways', 'means', and 'ends'.[12] To recap, in its entirety IE encompasses: firstly, intelligence-associated collection/gathering and analysis/assessment (estimate) work; to secondly, the further operationalised implementation of plans and intents generated by commanders and other high-level leaders and policy- to decision-makers.[13]

Several different stakeholders are involved. When thinking with regard to the conduct of many purposed multi-functional to special operations during an overall era of globalised strategic risk, several 'edges' naturally benefit from their 'extra sharpening' to gain advantage: for example, as can readily be acknowledged in competitive terms, such as acquiring and maintaining the initiative or 'upper-hand' over adversaries and rivals - see also, for example, in relation to the previously referenced case of the contemporary fight against so-called Islamic State in the Middle East and elsewhere across the World.[14]

---

[10] These different steps are detailed throughout Chapters 3 and 4 of *Ibid.*

[11] See as summarized in 'Figure 4.6. Overview/Summary', as published in Svendsen, *Intelligence Engineering* at the bottom of p.91.

[12] As highlighted in D.S. Reveron and J.L. Cook, 'From national to theater: Developing strategy', *Joint Forces Quarterly - JFQ*, 70 (2013), pp.113-20.

[13] See, especially, Svendsen, *Intelligence Engineering*, p.21, pp.61-62, pp.72-73.

[14] For more on 'gaining-the-initiative' insights, see as articulated in, e.g., A.D.M. Svendsen, *The Professionalization of Intelligence Cooperation: Fashioning Method Out of Mayhem* (Basingstoke, UK: Palgrave Macmillan, 2012), p.17; see also A.D.M. Svendsen, 'Intelligence, Surveillance and Reconnaissance' in D. Galbreath and J. Deni (eds), *The Routledge Handbook of Defence Studies* (London: Routledge, 2018), pp.275-6 and p.280.

Currently, Intelligence Engineering is representative of a very much continuing to evolve work-in-progress. Many parts continue to be worked out in the entirety of their details. IE should retain that status of remaining a 'work-in-progress'. This is in order to adequately maintain the sustained (extending to sustainable) delivery of its end-user (customer, client or consumer) STARC criteria, relating to being: Specific, Timely, Accurate, Relevant and Clear. IE overall considerably reflects the operational parameters that would naturally be expected with such a developing entity unfolding along the lines and in the directions as just characterised.[15]

Further insight is available. IE can also be regarded as being substantially strategic, classroom and workshop-orientated at present - for example, this present configuration is to encourage more 'off-line'-related modes of constructive *critical thinking*, such as 'outside', even 'beyond', 'the box', offsetting less-reflective and reflexive 'no time to think' push-and-pull pressures.[16]

Arguably, into the future, to further extend its current capabilities, the IE approach would benefit from greater automation and from better harnessing 'Big Data' to 'data intelligence' or DATINT inputs in its overall calibration to become even more instantly and operationally relevant. This is so that IE to all of its fusion potential can be used more effectively and efficiently in higher-tempo environments - for instance, relating to the improved collection and gathering to analysis and assessment of data in variously configured operational to battlespaces (whether they are multi-functional or special, see above).[17] Different 'intelligence cycles' involving a series of processes going from 'data' to 'information', 'information' to 'intelligence', and 'intelligence' to 'knowledge', similarly gain via Intelligence Engineering and its more explicit mobilisation.[18]

---

[15] For more on the STARC criteria, see Svendsen, *Intelligence Engineering*, p.143, col.2; see also A.D.M. Svendsen, '"Work-in-progress"? Revisiting the UK Serious and Organised Crime Strategy of 2013 and surveying UK efforts against transnational organised crime', *RUSI Strategic Hub for Organised Crime Research (SHOC) - The Informer blog* (8 November 2017).

[16] See also the different 'modes' or 'systems of thinking' as discussed throughout D. Kahneman, *Thinking, Fast and Slow* (London: Allen Lane, 2011); see also Svendsen, *The Professionalization of Intelligence Cooperation*, p.144; Svendsen, *Intelligence Engineering*, p.102.

[17] Again, see for example as advanced throughout, *ibid.* - including in relation to the so-called Islamic State (IS/ISIS/ISIL/Daesh) and cyber intelligence (CYBINT) mini-case study examples presented over pp.68-69; see also *ibid.*, p.74 and p.102; M.B. Ainsworth, 'Embracing analytics: A path forward for the intelligence community', *SAS Voices blog* (15 September 2017).

[18] Svendsen, *Intelligence Engineering*, p.39.

Conclusions

Through its arrangement as introduced and advanced throughout this article, Intelligence Engineering effectively captures and then addresses the complexity of the '*multi-everything*' nature of operational-to-strategic environments.[19] As already suggested, this is for the multi-functional purposes of (amongst other aims): 'M4IS2: multiagency, multinational, multidisciplinary, multi-domain information sharing and sense making'. Those activities also range across and involve the 'eight entities [of] commerce, academic, government, civil society, media, law enforcement, military and non-government/non-profit' organisations.[20] From these insights so configured, business and enterprise relevance becomes increasingly self-evident.

By pursuing its different steps with adequate due diligence across suitably defined timeframes and locations, IE work helps (1) find and fill the 'gaps' and/or mitigate so-called 'missing dimensions', (2) better address instances of so-called 'cognitive dissonance', as well as (3) helps to 'join/connect-the-dots' in and across all domains of operational-to-strategic activity that span from Human and Information to Sea, Air, Land, Space and Cyber(space).[21]

Furthermore, the Intelligence Engineering tools and frameworks extending to their related concepts as presented throughout this article, help us move across several knowledge domains, from: (i) merely exploiting KNOWN-KNOWNs ('what we know we know'); to (ii) exploring KNOWN-UNKNOWNs ('what we know we do not know'); to (iii) exposing UNKNOWN-KNOWNs ('what we do not know we know'); and to (iv) discovering (potential) UNKNOWN-UNKNOWNs ('what we do not know we do not know') areas.[22]

As the following list demonstrates, this intelligence up and across to knowledge work is useful for a further extensive catalogue of tasks, extending from: (a) operational-to-strategic early warning; (b) over-the-horizon insights; (c) better keeping 'ahead of the curve of events and developments'; (d) distinguishing (weak-strong) 'signals' from (overall/background) 'noise';

---

[19] 'Figure 3.2 - Geospatially Oriented Aspects of the Information Domain of the Operating Environment', published in E.V. Larson, *et al.*, *Assessing Irregular Warfare: A framework for Intelligence Analysis* (RAND, 2008), p.25.

[20] G. Segell, 'Book review: *International intelligence cooperation and accountability*', *Political Studies Review*, 10, 3 (2012), pp.410-11; Svendsen, *Intelligence Engineering*, p.3 and p.66.

[21] For a useful illustration, see the figure titled: 'Cross Domain Synergy: Campaign planners can understand the complex environment by considering each domain and its effects on others', as published in *PRISM*, no.3 (2016), p.16; see also, e.g., via Svendsen, *Intelligence Engineering*, p.136, col.2.

[22] Svendsen, *Intelligence* Engineering, p.73, pp.92-93; see also A.D.M. Svendsen, 'Discovering "unknown-unknowns" & beyond', *Conference paper presented at the 33rd International Symposium on Military Operational Research (ISMOR)*, Royal Holloway, University of London (July 2016).

(e) maintaining the 'edge' and 'initiative'; and (f) for better filtering, targeting, prioritisation, and so forth (again, *whatever* the precise context confronted).[23]

Offering assistance for answering the critical questions of 'So What?' and 'why does this matter?' or 'why should we care?', IE provides added value and USPs contributing towards, firstly, 'intelligence optimisation' tasks (IE analytical input), and then, secondly, 'best event and development transformation' such as through shaping and better situation to event and development awareness and framing to nudging and steering (involving more explicit IE engineering input). This last work is undertaken for the purposes of tailoring most advantageous opportunities and possibilities into the future. All-important *harm prevention* is simultaneously encouraged by these more conscientious activities and thereby improved.

Arguably, Intelligence Engineering responds equally well to critique. Perhaps in the remit of its ambition(s), IE even offers us at least beginning steps towards the 'holy grail' in (at least) Intelligence Studies of a 'grand(er) theory' of intelligence?[24] Granting not only greater intellectual potential that theoretical work can then be realised more practically in action through its greater application and harnessing, using IE as at least a guide for pathways ahead: 'Going forward, the intelligence theorist can learn much from the intelligence engineer, and vice versa.'[25] Ultimately, through mechanisms such as Intelligence Engineering and its extended implementation, contemporary defence and security efforts can be viably improved for better operating beyond the boundaries of the conventional. Difference is created.

* * *

ACKNOWLEDGEMENTS:

The author would like to thank Dr. Stephen Coulthart for his valuable feedback after the presentation of a draft of this article during a panel at the *Intelligence in the Knowledge Society (IKS) Conference 2017*, held in Bucharest, Romania (October 2017), as well as thank an anonymous reviewer for their helpful comments.

---

[23] See, e.g., as discussed in A.D.M. Svendsen and M. Kruse, 'Foresight and the Future of Crime: Advancing Environmental Scanning Approaches', chapter in H.L. Larsen, J.M. Blanco, R. Pastor Pastor, & R.R. Yager (eds.), *Using Open Data to Detect Organized Crime Threats: Factors Driving Future Crime* (London: Springer, 2017); Svendsen, *Intelligence Engineering*, pp.92-94.

[24] See, e.g., C. Hillebrand and R.G. Hughes, 'The Quest for a Theory of Intelligence', ch. 1 in R. Dover, H. Dylan, M. Goodman (eds.), *The Palgrave Handbook of Security, Risk and Intelligence* (London: Springer, 2017), pp.1-24.

[25] Svendsen, *Intelligence Engineering*, p.106.

References:

1. Ainsworth, M.B., 'Embracing analytics: A path forward for the intelligence community', *SAS Voices blog* (15 September 2017).

2. Eriksson, G., Pettersson, U., (eds.), *Special Operations from a Small State Perspective: Future Security Challenges* (London: Springer, 2017)

3. Hillebrand, C., Hughes, R.G., 'The Quest for a Theory of Intelligence', ch. 1 in R. Dover, H. Dylan, M. Goodman (eds.), *The Palgrave Handbook of Security, Risk and Intelligence* (London: Springer, 2017), pp.1-24.

4. Kahneman, D., *Thinking, Fast and Slow* (London: Allen Lane, 2011); see also Svendsen, *The Professionalization of Intelligence Cooperation*, p.144;

5. Kwa, C.G., 'Postmodern Intelligence: Strategic Warning and Crisis Management', chapter in F. Baudet, E. Braat, J. van Woensel, A. Wever (eds.), *Perspectives on Military Intelligence from the First World War to Mali: Between Learning and Law* (London: Springer, 2017), pp. 97-118;

6. Larson, E.V., *et al.*, *Assessing Irregular Warfare: A framework for Intelligence Analysis* (RAND, 2008), p.25.

7. Madureira, L., 'Market and Competitor Analysis: Real Exercise', ch. 8 in W.J. Lahneman and R. Arcos (eds), *The Art of Intelligence* (NY: Rowman & Littlefield, 2014), p.133;

8. Pherson, R.H., Pyrik, John, *Analyst's Guide to Indicators* (US: Pherson Associates, LLC, 2017).

9. Reveron, D.S., Cook, J.L., 'From national to theater: Developing strategy', *Joint Forces Quarterly - JFQ*, 70 (2013), pp.113-20.

10. Segell, G., 'Book review: *International intelligence cooperation and accountability*', *Political Studies Review*, 10, 3 (2012), pp.410-11;

11. Svendsen, A.D.M., 'Developing international intelligence liaison against Islamic State: Approaching "one for all and all for one"?', *International Journal of Intelligence and CounterIntelligence*, 29, 2 (2016);

12. Svendsen, A.D.M., *The Professionalization of Intelligence Cooperation: Fashioning Method Out of Mayhem* (Basingstoke, UK: Palgrave Macmillan, 2012), p.17;

13. Svendsen, A.D.M., 'Intelligence, Surveillance and Reconnaissance' in D. Galbreath and J. Deni (eds), *The Routledge Handbook of Defence Studies* (London: Routledge, 2018), pp.275-6 and p.280.

14. Svendsen, A.D.M., "Work-in-progress"? Revisiting the UK Serious and Organised Crime Strategy of 2013 and surveying UK efforts against transnational organised crime', *RUSI Strategic Hub for Organised Crime Research (SHOC) - The Informer blog* (8 November 2017).

15. Svendsen, A.D.M., 'Discovering "unknown-unknowns" & beyond', *Conference paper presented at the 33rd International Symposium on Military Operational Research (ISMOR)*, Royal Holloway, University of London (July 2016).

16. Svendsen, A.D.M., Kruse, M., 'Foresight and the Future of Crime: Advancing Environmental Scanning Approaches', chapter in H.L. Larsen, J.M. Blanco, R. Pastor

Pastor, & R.R. Yager (eds.), *Using Open Data to Detect Organized Crime Threats: Factors Driving Future Crime* (London: Springer, 2017);

17. Svendsen, A.D.M., (2017), *Intelligence Engineering: Operating Beyond the Conventional* (New York: Rowman & Littlefield / Security & Professional Intelligence Education Series - SPIES, 2017).

18. Svendsen, A.D.M., (2015), 'Advancing "defence-in-depth": Intelligence and systems dynamics', *Defense & Security Analysis*, 31, 1 (2015), pp.58–73.

19. Svendsen, A.D.M., (2015), 'Contemporary intelligence innovation in practice: Enhancing "macro" to "micro" systems thinking via "System of Systems" dynamics', *Defence Studies*, 15, 2 (2015), pp.105–23.

20. Svendsen, A.D.M., 'Brexit: an agent of "disruptive change" for UK and European intelligence?', *Journal of Intelligence History* (2017).

21. Svendsen, A.D.M., 'Strategic Futures and Intelligence: The Head and Heart of "Hybrid Defense" Providing Tangible Meaning and Ways Forward', *Small Wars Journal - SWJ* (June 2017).

22. 'UK launched cyber-attack on Islamic State', *BBC News* (12 April 2018).

OPEN SOURCE INTELLIGENCE (OSINT)

DATA ANALYSIS VERSUS INTELLIGENCE ANALYSIS: WHAT'S NEW IN THE GAME?

Andrada Nicoleta HALGAŞ - BLAGA*

Abstract

Nowadays, when information is abundant, ever-present and readily available, how does an intelligence organization adapt, in order to collect and process what is truly relevant, as well as provide "value-added" to decision-makers?

The information revolution has greatly impacted national intelligence. Collection has become increasingly focused on large sets of data (big data). As more of that processed data is available outside intelligence organizations, the role of intelligence professionals has shifted from analysing collected data to provide assessments of current events, to that of generating knowledge, predictions and warning that help decision-makers avoid strategic surprises.

Keywords*: data analysis, intelligence analysis, big data, analysis-driven collection, data analysis tools, tech skills, research and development, artificial intelligence*

Data and Intelligence analysis - Elements of difference and continuity

There is little consensus so far regarding the definition of data analysis. This is probably due to the fact that data analysis is traditionally closer to business intelligence, which means it hasn't until recently been the focus of IC research efforts in order to properly delineate it from similar concepts such as *data science* or *machine learning*.

In order to better understand our topic of discussion, let's take a look at the following definitions:

Data: 1. Facts and statistics collected together for reference or analysis (Oxford Dictionaries).

1.1 The quantities, characters or symbols on which operations are performed by a computer, which may be stored or transmitted in the form of

* Analyst, intelligence research and development specialist.

electric signals and recorded on magnetic, optical, or mechanical recording media (Oxford Dictionaries).

Intelligence: As in the case of data or data analysis, there have been several attempts to define intelligence, in the context which is of interest here. Seven years later, Michael Warner's words on the issue still hold and a definition of intelligence remains on the "Wanted" list of intelligence professionals worldwide (Warner, 2007).

Several of the most meaningful definitions, for the points further made in this paper, are as follows:

1. [Intelligence is] knowledge or foreknowledge of the world around us - the prelude to decision and action by US policymakers (Central Intelligence Agency, 1999).

2. On the one hand, it [intelligence] refers to organization collecting information and on the other to the information that has been gathered (Lauquer, 1985).

These two definitions lead to the conclusion that the common understanding among intelligence professionals is that intelligence is both a process and the product resulting from it, and that its purpose is to assist decision-makers in adopting policies.

Analysis:

1. Breaking down a problem into its component parts, assessing each part separately, then putting the parts back together to make a decision (Heuer).

2. The conversion of processed information into intelligence through the integration, evaluation, analysis, and interpretation of all source data (US Department of Defence).

If we take into consideration only the first acceptation of data provided by the Oxford Dictionary, then we have nothing new in the game of data analysis, compared to intelligence analysis: they both mean collecting and processing pieces, providing them with context and meaning and delivering the full puzzle to decision-makers.

However, if we look at the second definition of data, we may observe that there is a third party involved: the **computer**. In this case, data analysis implies a different sort of process, technology being a key element of it. Data is defined as "quantities, characters or symbols", which hints at the fact that before processing them by using specialized software, they might not be intelligible to the intelligence analyst. If in the first case, "facts" and "statistics" can be analysed even without the help of technology, for "quantities, characters or symbols", software processing is a prerequisite.

Therefore, we may conclude that data analysis is, in fact, based on the same principles as classical intelligence analysis, the main difference being that it has a greater quantitative dimension and it might (and almost always does) need specialized processing technological tools. Historically speaking, it is a product of the information age. In order to better follow this line of reasoning, let's take a look at Edward Waltz's timeline on the evolution of intelligence:

Age	**Agricultural**	**Industrial**	**Information**	
Approx. Period	**Until–1700**	**1700–2000**	**2000–Future**	
Wealth Creation: Power and Business	*Method: peasant-based crop production Resource: land*	*Method: mass production of goods Central resource: raw materials*	*Method: customized production of knowledge services Central resource: knowledge*	
Nation-State Warfare, Conflict, and Competition	*Object of conflicts: land Infantry warfare: attrition of infantry (target human bodies)*	*Objects of conflict: regional economies, access to materials Mechanized warfare: mass destruction of weapons (target mechanized weapons)*	*Objects of conflict: global economies, ideologies Information warfare: attrition of will and capability, precision targeting, speed and agility, management of perception (target the human mind)*	
Focus of Intelligence	*Human collection centric (covert access)*	*Technical sensing centric (remote access)*	*Network centric (network access)*	*Knowledge - centric (perceptual access)*
Intelligence Examples	*Moses, Sun Tzu, General George Washington*	*World War II: radio, radar, cryptography; use of air platforms Cold War: space reconnaissance*	*Post–Gulf War: emphasis on network-centric warfare, battlefield digitization, rapid targeting and data dissemination*	*Future emphasis on human cognition, decision-making and influence*

Table: Edward Waltz's timeline on the evolution on intelligence (Waltz, 2003)

What we learn from the above timeline is that starting with the industrial revolution, the traditional meaning of *intelligence* (analysed information obtained through secret means, based on human collection and covert access) has been expanded to encompass information obtained through technical, remote access sources. The specific difference here is that the data obtained through technical means is, in most cases, not directly intelligible to the customer. It needs processing before it can be transformed into an intelligence product, which adds an extra layer of primary analysis, consisting of the "translation" of the data into something that can be read and further evaluated. Then came the information revolution, and with it, a further expansion of the meaning of *intelligence.* The main issue here is not necessarily adding an extra layer of processing (although that, too, is the case), but an extra layer of *meaning,* of analytic input and evaluation.

The element of continuity throughout this series of evolutions is the main purpose of intelligence, which remains providing the customer with valuable insight that could not be obtained through other means.

There is a lot of buzz these days around **big data**, so much so that skeptics argue it is in fact a concept devoid of meaning, since data has always been big, in comparison to the collection possibilities of its corresponding time. As data gets bigger, so does the capacity of collection and processing tools. Indeed, just like data analysis, big data eludes a commonly accepted definition. However, since it is beside the point to make an inventory of its different understandings, we'll go with Schutt and O'Neil's definition: data is considered "big" when you can't fit (and process) all of it on one machine (Schutt & O'Neil, 2014). Why is the growing size of data relevant to intelligence, however?

The view of the author of this paper is that when considered in the context of national intelligence, data analysis is a blend of quantitative and qualitative research. Data analysis as we understand it now has as a main object evaluating **large chunks of computer-processed quantitative data**, and providing interpretations of it based on qualitative indicators, which can stem from **substantive expertise** in the field of research, the only input powerful enough to provide crucial insights into interpreting quantitative data.

It is clear that human expertise is still very much needed in order to select what's relevant and what should be further analysed. Of course, this was also the case when data was not that big yet, but its growing size poses a

correspondingly growing problem for analysts. Software that selects data making use of key indicators is of course available on the market, but experience has proven that automatically selected data is still far lower in quality and relevance than data selected by humans.

Researchers hope this technical glitch might be solved with the development of **artificial intelligence** (AI), but experiments conducted so far have proven that what humans consider relevant is not regarded in the same way by bots. An AI experiment by Facebook, for instance, was allegedly shut down after the bots started developing their own language, unintelligible to humans (unless linguistically analysed). The researchers assumed that the bots did this because they found human language sequences irrelevant to the tasks they were required to perform. On the other hand, the data scientists that were conducting the experiment called the newly-developed language "functional gibberish" and considered it inefficient (Quora, 2017).

Whatever the real reason behind Facebook pulling the plug on its AI program, one thing remains clear: bots and humans don't speak the same language yet. So if we can't put our faith in AI, what's the solution to our collection-selection-analysis issues?

The impact of big data on intelligence processes, products and human resources

- ***Analysis-driven collection: the solution to smart, efficient collection & processing in the age of big data***

The traditional intelligence cycle begins with planning, and up to a certain point, this still holds. When we think of planning what to collect, what were traditionally taken into account were the issues of national interest which stemmed from previous collection efforts. This is commonly known as **issue-driven collection**, an efficient way of organizing intelligence collection when data was a bit smaller, and definitely not as publicly available. However, issue-driven collection in the information age has led to a set of problems, including collecting more than can be processed, difficulties in ensuring the timely and correct selection of relevant data out of large data sets and the ethical issue of possibly collecting more than can be objectively justified.

The Joint Inquiry into the performance of the US Intelligence Community after the events of 9/11 concluded, among other things, that

the nation's greatest collector, the NSA, had very little time at its disposal to actually process and further select and analyse all the input it got daily. This was found to be the reason why a relevant lead to the future attacks was only processed a few days after the event (House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, 2002).

One of the reforms that took place afterwards was shifting towards **analysis-driven collection**, which is, in fact, a mere recognition of the fact that "collection priorities should reflect the needs of those crafting the analysis, who depend upon the collected intelligence" (Lowenthal, 2016). According to the former DDNI-A, Thomas Fingar, analysis-driven collection actually worked for the American IC, leading, among other things, to more focus from collectors on providing information that would lead analysts to crucial insights, and thus, making selection at least a bit easier (Fingar & Graham, 2010).

- ***Packaging and "selling" intelligence products***

In the present age, information (processed and analysed information, even) is literally everywhere. The massive development of OSINT has had a great contribution to this, since it gave rise to many different entities collecting and analysing public information in order to aid the decision-making process at different levels.

Therefore, for the first time in history, national intelligence became a business that had to compete for its' customers attention and time. Of course, even traditional intelligence products went by tradecraft standards that required them to be attractive and attention-catching, but this usually still only meant that analysts had to pay attention to their writing, since this was their fundamental skill.

Intelligence professionals today are not only concerned with gaining substantive expertise and mastering analytic tradecraft, but also with learning and implementing marketing principles, adapting to different platforms of putting their information forth and learning new, complex skills that go way past the ability to write well, in order to make their intelligence products or services attractive to decision-makers.

Regarding this issue, Ruben Arcos and Randolph Pherson make an excellent point on the rising necessity for analysts to acquire multimedia competencies, in order to better fit the current intelligence market and keep up with today's customers (Arcos, 2015).

- ***The role of the data analyst in the intelligence organization***

Speaking of skills, let us further discuss an altogether new position in the intelligence organization: the data analyst. What sort of creature should she or he be, and what are the corresponding roles to fill? There are, of course, many possible answers to this question. First of all, a data analyst is the person whose job is first-level processing of "quantities, symbols and characters" (which are mostly collected through technical or open sources). She or he must be an expert in the corresponding source of collection, in order to be able to process the collected data by making use of the appropriate software. After this initial stage of "translation", the data analyst selects and analyses the previously processed single-source data by assigning it source and information credibility, in accordance with the Admiralty code or whatever else single-source analysis scale the intelligence organization uses.

The resulting data report, translated into an intelligible form and assigned credibility, is further passed on to the **intelligence analyst,** whose role is to put together such reports from all collection sources, provide an evaluation by interpreting quantitative data in qualitative ways, and transform them into deliverable intelligence products.

This, however, is not the only application of data analysis in an intelligence context. Some types of data can be further processed through statistical modelling, and in such cases, they can also provide support at an operational level:

- **User-level modelling** is the process behind the so-called "online bubble" we all live in. Our online behaviour is constantly being scrutinized, stored and analysed through cookies, which ads companies or social media further use in order to provide us with online content that suits our preferences and interests. In a similar manner, data analysts can use publicly available market research statistics or data obtained from the analysis of social media behaviour in order to profile potential HUMINT sources or to target and monitor individuals that may pose security threats.

- **Population-level modelling** - In business intelligence, one of the main functions of data analysis is to aid decision-makers in establishing and carrying through their marketing and lobbying strategies. The same process of subtly influencing the collective narratives people believe in is employed by secret services or governments, in order to manipulate public opinion. In a TED Talk regarding Russian propaganda, cyberspace analyst Laura Galante describes the process through which data can be modelled and used in order

to erode the very core of the values we believe in, such as democracy or human rights (Galante, 2017).

The reversed process, which can easily be modelled through data analysis, can be of great use in counterintelligence efforts that aim to discover and prevent the enemy from projecting influence through information operations.

Conclusions

The current unprecedented technological advancements have provided intelligence organizations with an important asset: the ability to collect and process large amounts of data. However, the same changes have also given rise to a set of issues that need to be addressed. Modern intelligence organizations can no longer function in a traditional logic; they **need to adapt their processes, products and people**.

1. Big data, little processing - Intelligence organizations collect larger amounts of data than they can process, or, even better said, more than is truly needed.

Solution*: A full shift from issue-driven towards analysis-driven collection is necessary, for the following reasons:*

- to better organize the collection-analysis process;

- to ensure a higher quality input from collectors;

- to allow for more focus on strategic rather than current analysis.

2. Better tools and people who can use them - The 21'st century intelligence analyst is a substantive expert, a master of tradecraft and a proficient multimedia user. Moreover, today's challenges create new positions within intelligence organizations for tech savvy people, needed in order to bridge a current expertise gap.

Solution: *Apart from expanding the recruitment pool for potential candidates, intelligence organizations ought to make sure IC data and intelligence analysts are constantly connected to the best and newest research and training in their field, which means establishing a better and more solid connection with outside experts.*

Intelligence R&D has a key role here, both through providing the sets of requests for the development of software and analytic tools, as well as through being in constant contact with the world outside and its experts.

References:

1. Arcos, R. (2015). Multimedia competencies and the intelligence analyst. In R. Arcos, & R. H. Pherson, Intelligence Communication in the Digital Era. Transforming Security, Defence and Business (pp. 15-16). Palgrave Macmillan.
2. Center For Security Studies. (2007). Emerging Threats in the 21st Century: Strategic Foresight and Warning Seminar Series Final Report. Zurich.
3. Central Intelligence Agency (Office of Public Affairs). (1999). A Consumer's Guide to Intelligence. Washington DC: Central Intelligence Agency.
4. Fingar, T., & Graham, M. M. (2010, April). Five years later, a stronger intelligence community.
5. Galante, L. (2017, April). How (and why) Russia hacked the US election. Retrieved September 16, 2017, from Ted Talks: https>//www.ted.com/talk/laura_ galante_how_to_exploit_democracy
6. Heuer, R. (1999). Psychology of Intelligence Analysis. Centre for the Study of Intelligence. Retrieved from www.odci.gov/csi/pubs.html
7. Heuer, R. (2013). Limits of Intelligence Analysis. Retrieved from www.iwp.edu/docLib/20131120_HeuerLimitsofIntelligenceAnalysis.pdf
8. House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. (2002). Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001.
9. Krizan, L. (1999). Intelligence essentials for everyone. National Intelligence Meets Business Intelligence. Washington DC. Retrieved mai 4, 2017, from www.strategyawareness.com
10. Lauquer, W. (1985). A World Of Secrets: The Uses and Limits of Intelligence. New York: NY: Basic Books.
11. Lowenthal, M. M. (2016). Intelligence. From Secrets to Policy. CQ Press.
12. National Security Agency USA. (n.d.). Operations Security - Intelligence Threat Handbook. USA. Retrieved august 19, 2017, from https://fas.org/irp/nsa/ ioss/threat96/part02.htm
13. Office of the Director of National Intelligence USA. (n.d.). What is Intelligence? Retrieved august 19, 2017, from https://www.dni.gov/index.php/what-we-do/what-is-intelligence
14. Oxford Dictionaries. (n.d.). Retrieved September 14, 2017, from en.oxforddictionaries.com/definition/data
15. Quora. (2017, August 16). Why Facebook Shut Down its AI Program That Went Rogue. Retrieved September 16, 2017, from Forbes: www.forbes.com/sites/ quora/2917/08/16/Why- Facebook- Shut- Down- its- AI- Program- That- Went-Rogue/#322a5ae1710

16. Schutt, R., & O'Neil, C. (2014). Doing Data Science. Straight Talk from the Frontline. O'Reilly Media, Inc.

17. Waltz, E. (2003). Knowledge Management in the Intelligence Enterprise. Artech House Information Warfare Library. Retrieved from https://phamtrung.wikispaces.com/file/view/KMinIntelligentEnterprise.pdf

18. Wark, W. K. (2009). Secret Intelligence: A Reader. In R. J. Aldridge, Secret Intelligence: A Reader (p. 528). Routledge.

19. Warner, M. (2007, April 14). Wanted: A Definition of Intelligence. Understanding our Craft. Retrieved from Central Intelligence Agency: www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html#fn7

HISTORY AND MEMORY IN INTELLIGENCE

THE ROMANIAN SECRET SERVICE (SSI): FROM AGENT TO HUMINT COLLECTOR

Bogdan Alexandru TEODOR[*]

Mihaela TEODOR[**]

Abstract

Talent or human capital is the most important single factor that determines business success or failure. In this respect, the topic of Human Intelligence (HUMINT), or what is more popularly referred to as people, talent, human capital, was and remain one of the hottest topic of the intelligence history. Today, HUMINT may be defined as the collection of information by a trained HUMINT collector, from people and their associated documents. During the entire interwar period, the chief of Romanian Secret Service (SSI) strived to introduce modern principles for conducting the Romanian intelligence activity, as archival documents state. One of the modern principles applied was the permanent concern for recruitment of human sources or agents. Having in mind the contemporary definition of HUMINT, this paper aim to provide a historical perspective on the Romanian Interwar Secret Service's policy of recruitment, trying to identify inside the structure of the SSI the defining elements of intelligence.

Keywords*: intelligence, agent, HUMINT collector, Romanian Secret Service, interwar period*

Introduction

The role of the Romanian intelligence services from the interwar period, as well as their structural evolution and main areas of activity were

[*]Associate Professor Dr. within "Mihai Viteazul" National Intelligence Academy, teodorbogdanalexandru@gmail.com

[**] Researcher Dr. within National Institute for Intelligence Studies, "Mihai Viteazul" National Intelligence Academy, teodor_mihaela@yahoo.com

closely connected to the domestic and foreign risk factors.[1] To cope with the challenges, during the entire interwar period, the chief of Romanian Secret Service (SSI) strived to introduce modern principles for conducting the Romanian intelligence activity, as archival documents state. One of the modern principles applied was the permanent concern for recruitment of human (re)sources or agents, being generally accepted that talent or human capital is the most important single factor that determines business success or failure.

Starting with the contemporary definition of HUMINT collector, used by military intelligence field manuals or intelligence dictionaries, this paper aim to provide a historical perspective on the Romanian Interwar Secret Service's (SSI) policy of recruitment, trying to identify inside the structure SSI the defining elements of intelligence. First, we will define the terminology used for the purpose of our study. After a short presentation of the changes occurred in intelligence field during the Great War, we will examine the Secret Service's archival documents in order to identify which was the recruitment policy and what were the characteristics of intelligence agents and if there is a similarity with the characteristics of the HUMINT collector.

What means what! The term "agent" was often used in the intelligence literature to refer both to officers and the people they recruited or sources, which can often be confusing. According to the contemporary intelligence dictionaries, "the agent is a person unofficially employed by an intelligence service, often as a source of information" (*Language of espionage*). The same contemporary literature refers to the person recruiting the agent as either "officer" or "case officer". In accordance with the Romanian archive documents used in this research as main sources, we will use the term "agent" to refer to the person being recruited and employed by the Intelligence structure to obtain secrets or carry out covert activities (Suvorov, 1984).

---

[1] A version of this article has already been published as Bogdan TEODOR, Mihaela TEODOR, *The Great War and the Romanian military intelligence structures: changes in the recruitment policy,* în The 14th International Scientific Conference "Strategies XXI". Strategic Changes in Security and International Relations, Vol. 2, eds. Gheorghe Calopăreanu, Iulian Martin, Constantin Popescu, Ioana Enache, Gelu Alexandrescu, Daniel Ghiba, Marius Serbeszki, „Carol I" National Defence Univeristy Publishing House, Bucharest, April 26-27, 2018, pp.184-194, ISSN 2285-8415, accessible on-line at https://www.strategii21.ro/A/2018-04.%20STRATEGIC%20CHANGES%20IN%20SECURITY%20AND%20INTERNATIONAL%20RELATIONS/Security%20and%20Defence%20Faculty%20Vol%202%20Strategic%20changes%20in%20security%20and%20international%20relations%202018.pdf

The Human Intelligence Collector, commonly referred to as HUMINT, provide Army leaders with vital information about enemy forces, dispositions, plans, tactics, strengths, and weaknesses, as well as detailed information about the battlefield (*U.S. Army Human Intelligence Collector Field Manual,* 2015). HUMINT may be defined as the collection of information by a trained HUMINT collector, from people and their associated documents (press, letters, official documents etc.) (*Human Intelligence Collector Operation,* 2006, p. 22; *U.S. Army Human Intelligence Collector Field Manual,* 2015).[2]

HUMINT includes overt, sensitive, and clandestine activities and the individuals who exploit, control, supervise, or support these sources (Air Force Pamphlet, 1990). HUMINT collectors, conduct screenings, interrogations, and debriefings of civilians on the battlefield, prisoners of war and detainees to collect information, participate in intelligence gathering operations; draft intelligence reports (*U.S. Army Human Intelligence Collector Field Manual,* 2015).Therefore, HUMINT activities require significant time to identify and develop potential sources of information. HUMINT collectors interact with and question other human beings and will often be a qualified linguist in the target area language. Based upon these skill sets, commanders may assign HUMINT collectors missions similar to activities often associated with civil affairs, criminal investigative command, or interpreters or translators (*Human Intelligence Collector Operation,* 2006, p. 20).

A HUMINT source is a person from whom information can be obtained. Potential HUMINT sources include threat, neutral, and friendly military and civilian personnel, as stressed *The Stratford Glossary of Useful, Baffling and Strange Intelligence Terms*. Categories of HUMINT sources include but are not limited to detainees, refugees, local inhabitants, friendly forces, and members of foreign governmental and non-governmental organizations (*Human Intelligence Collector Operation,* 2006, p. 22).

As we stressed already, based on definition of HUMINT collector, this paper aims to provide a historical perspective on the Romanian Interwar Secret Service's policy of recruitment, trying to identify inside the structure of SSI the defining elements of HUMINT collector and to prove that the Romanian Intelligence Service from interwar period was a modern one.

---

[2]Acording to the *U.S. Army Human Intelligence Collector Field Manual*, 2015,`HUMINT is the collection of information by a trained HUMINT collector (military occupational specialties [MOSs] 97E, 351Y [formerly 351C], 351M[formerly 351E], 35E, and 35F), from people and their associated documents and media sources to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities. It uses human sources as a tool and a variety of collection methods, both passively and actively, to gather information to satisfy the commander's intelligenc requirements and cross-cue other intelligence disciplines`.

The Great War and the Romanian intelligence structures

Researchers agree that the Great War changed modern warfare, military intelligence evolving as a significant force arm in most of the participating countries. Moreover, most of national intelligence structures were forced to rapidly modernize, revising espionage and intelligence tradecraft to fit changing battlefield tactics and technological advances. At the outbreak of the war, many nations had weak or fledgling national intelligence communities. Thus, the experience of the war formed the first modern intelligence services, serving as forbearers of the intelligence communities in France, Britain, Germany, and Romania. [3] As Terrence J. Finnegan stressed in his research, when the war was over "many nations participating in the conflict realized the necessity for some sort of permanent intelligence services, or large government intelligence agencies" (Finnegan, 2009).

The situation of Romania during last period before the outbreak of World War I was extremely complicated[4]. The state was situated between two powers: Austria-Hungary and Russia. So, it had to conduct the policy of cautious balance, even if part of the Romanian political elites presented evident pro-German sympathies. However, in 1914, political and economic influences of Russia and France became much more effective than dynastic links with Germany. King Charles I Hohenzollern-Sigmaringen tried to argue about the necessity of Romanian access to the alliance with Central Powers in the context of Bucharest's aspirations for Bessarabia, but he had to accept the status of Romanian neutrality (see more in *Romania during First World War*, 1987, vol. 2). After the outbreak of European war, Romania tried to maintain the neutrality, officially declared on August 4th, 1914. This policy lasted to 1916, but in the atmosphere of regular diplomatic pressures from both sides of the conflict. However, key-events took place in August 1916. On August 17th Romania signed in Bucharest political treaty and military convention with Entente. Bucharest received guarantees of territorial integrity and promises of concrete compensations (Transylvania, Banat and Bukovina).

Thus, Romania entered the Great War, beginning military operations against Austria-Hungary on August 28th 1916. The Romanian Army was quite

---

[3] See more about the Frech intelligence at Eric Denécé, *Les Services de Renseignement et de Sécurité Français: perspective historique*, in "Note Historique", Centre Français de Recherchesur le Renseignement, no. 47, Novembre, 2016. Read more about British Intelligence on Nigel West (coord.), (2015), *Historical Dictionary of International Intelligence*, Second Edition, Rowman & Littlefield, New York – London. Read more about German Intelligence on Adrienne Wilmoth Lerner, *World War I. Encyclopedia of Espionage, Intelligence, and Security* available on-line on http://www.faqs.org/espionage/Vo-Z/World-War-I.html

[4] Read more about Romania and the Great War in: *Romania during First World War*, 1987, vol. 2; România în Marele Război. Testimonia available on https://ispaim.mapn.ro/pages/view/118.

large, with over 650,000 men in 23 divisions, but it suffered from poor training and equipment and lack of organized intelligence, particularly when compared to its German counterparts (*Romania during First World War*, 1987, vol. 2, pp. 832-833). At the front, the conservative military culture was forced to grapple with its tradition and make sense of combat in the new stationary environment. Concerning the Romanian military intelligence component, there was an Information Office within the General Headquarters (Bureau 5, Section III) which had in 1916 only 14 officers and some civilians as translators and designers (Spânu, 2012, pp. 202-211).

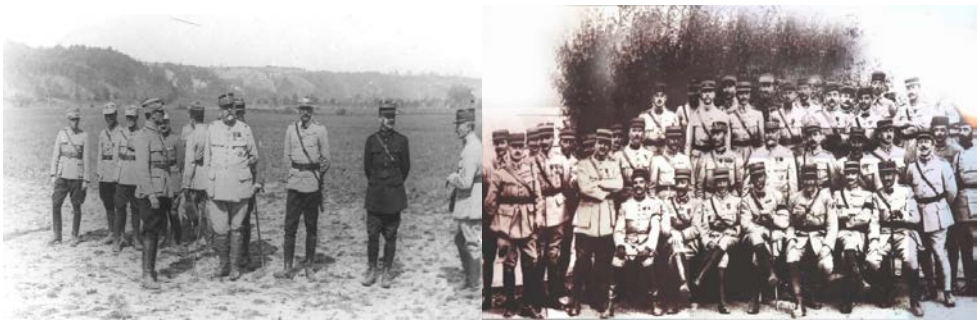
According to archive documents, the mission of the Information Office was to search, collect, and centralize information about the enemy by using various means: "secret agents behind the front lines, secret agents in the area of operations, military and civilian authorities at the border, and aerial recognition" (Spânu, 2012, p. 74). The secret agents sent behind the front lines should recruit informers and collect information about enemies' war preparations and population's mood. The secret agents sent in the area of operations should recruit informers and collect military information, and additionally they should act as counterespionage agents.

In practice the military intelligence structure does not look like that organized structure provided by the documents, as Col. Nicolae Condeescu, the future Head of the Information Section, states in his document from April 1918: "at the mobilization were set up information offices at Armies, Army corps and divisions, but were not prepared, did not exist officers well trained and doctrine. Instructions from head office could not be met easily." (Spânu, 2012, pp. 267-269) Thus, most of the archive documents stressed that at the beginning of 1916 the Romanian military intelligence structure was not very well organized, although officials talked about secret agents special trained for intelligence work and recruiting informers and spies with special funds provided by the army. Moreover, security agents from Direction of Police and General Security had to be seconded to the military units to carry out intelligence collection and counterespionage (Spânu, 2012, p. 74).

The lack of organization was reflected in the defeat suffered in the first part of the Romanian campaign with major repercussions on the military potential and combat capacity of the Romanian Armed Forces. During first months the Romanian forces broke into Transylvania on the depth 130 km, but there were first and last successes. On December 1916, allied forces entered to Bucharest, and the next year Germans and Austrians conquered southern Moldova and whole Wallachia (*Romania during First World War*, 1987, vol. 2). Romania suffered over 200,000 military casualties and two thirds of the country fell under a harsh occupation regime, the Government and the King had to retreat to Moldova.

Mărăşeşti battle.
Source: https://romaniadacia.wordpress.com/2014/11/16/for-the-heroes

In 1917, when both belligerent sides were making huge efforts to win the final victory, for Romania it was vitally important to rebuilt the Army in order to expel the occupying forces, since the existence of the Romanian state depended on it. Romania embarked on the reconstruction and strengthening of its combat capability during the first half of 1917 through multiple national efforts and allied help. The Romanian Army's reconstruction involved both re-organization and modernization, especially in terms of intelligence. The reorganization was initiated by King Ferdinand and the Romanian government. It was carried on under their leadership and control in the free national territory. A notable contribution to the reconstruction of the Romanian army was made by the 1,600-strong French military mission led by General Henri Mathias Berthelot (Tănase, 2015), which supervised the process and helped retrain Romanian troops.



French military mission led by General Henri Mathias Berthelot
Source: https://ro.wikipedia.org/wiki/Misiunea_Militar%C4%83_
Francez%C4%83_(1916-1918)

General Henri Berthelot, with a part of his mission colleagues[5], set up headquarters in Iaşi and became actively involved in solving tasks concerning cooperation with the representatives of the allied states.

The reorganization pursued the reduction of the effectives of the "Operations Army" to parameters that suited the country's resources for waging a long campaign. The infantry divisions were ensured identical structure to make replacements and maneuvers easier on the battlefront. The army corps became only a command body for tactical coordination. The cavalry divisions received more machine guns. The artillery material underwent a homogenization process, with two regiments for each division, while the heavy artillery was organized as a distinct group (*Romania during First World War*, 1987, vol. 2). Priority was given to trench warfare, the assimilation of new military technology and night combat. Considerable progress was achieved with the technical-material equipment of the army by means of its provisioning with armament, ammunition and other combat resources from inside the country, but even more importantly from abroad (*Romania during First World War*, 1987, vol. 2).

The reorganization also involved the other troops (combat engineers, air force, navy), and services as Information Service which underwent notable improvements with the help of French specialists. The directions, organization and methodology of the training of the command staff and the troops were considerably improved and special training centers were set up. Together with this corps of elite officers and technicians, General Henri Mathias Berthelot managed to inspire the Romanian army with the French methodical, clear spirit, as the *Deuxième Bureau* inspired the Romanian Secret Service.

Reorganization, emphasis on professionalism and continuity in intelligence work: from information officers to intelligence agents

If in the first months of the Great War the Romanian Intelligence proved not existed, in the battlefield, Romanian military leaders learned that access to accurate and timely information was essential to gain advantage in battle. After the Army reorganization, their command and control came to

[5] See more about the French military mission in Romania at Dumitru Preda, *Berthelot şi România/Berthelot et la Roumanie*, (1997), Bucharest: Univers Enciclopedic Publishing House; Petre Otu, *L'influence de la doctrine militaire française sur l'évolution de l'armée roumaine* (1878-1940), in "Revue historique des armées", no. 244 / 2006, pp. 28-49. Petre Otu (coord.), *Reforma militară şi societatea în România, de la Carol I a a doua conflagraţie mondială*, Occasional papers, Year 6, no. 8, 2007.

depend on constantly collected intelligence from a rapidly expanding list of sources and methods to support decisions from the planning stages to their execution.

Source: https://romaniadacia.wordpress.com/2014/11/16/for-the-heroes

For doing this, they accepted the creation of a permanent intelligence entity inside the Romanian Army, having as model the similar French regulation, as it was stated in the official document entitled *Instructions regarding the organization and functioning of the Intelligence Service* released on February 20, 1917 (Spânu, 2012, pp. 225-234; Spânu, 2010, pp. 117-118). There, we can find guidance on Service's organization principles, its recruitment policy and mission, and the first mention of the Secret Service. There was a special organization with responsibilities in "issues of both espionage agency and counterespionage" for which were issued special instructions on April 15, 1917: *Instructions on measures to be taken by Major Staff, services or army bodies in order to avoid indiscretions and guard us against enemy espionage*. (Spânu, 2012, pp. 235-237) According to this document, one of the innovations introduced in the organization of intelligence and counterintelligence structures was collecting intelligence by using nonofficial covers or secret agents permanent employees of the Secret Service, and trained personnel to centralize and exploit information gathered. Moreover, the document provide information about intelligence agents who must had morality and been trained to respect the principles on organization of the intelligence work as: conducting screenings, interrogations, and debriefings of civilians on the battlefield, prisoners of war and detainees to collect information, participate in intelligence gathering operations; partitioning and transmitting information in special conditions. Some of those characteristics we can identify in the list of HUMINT collectors definition.

Thus, we can state that it was about professionalizing the collecting information job, the information officer turning into intelligence agent.

At the same time the first document provide information about the prisoners or deserters interrogations as a principal mean to collect information about enemy used by Romanian intelligence agents (Spânu, 2012, pp. 230-231).We can already recognize some of the HUMINT collector characteristics: interrogations to be made only by intelligence officers and translators from intelligence offices of every army unit. As we know Human intelligence includes the most basic form of military intelligence, which is observation. In the Great War, and not only, Romanian soldiers at the front lines watched their enemies for details that might provide information on what the enemy is doing, as well as where and when and how fast.

By the summer of 1917, the Romanian Army stood on more equal ground with their enemies, in terms of intelligence work as specialists state. The results of the reorganization and modernization were visible, being confirmed in the great battles of the 1917 year. The work of the intelligence agents contributed to the three great battles, decisive for the Romanian nation's destiny, delivered at Mărăşti, Mărăşeşti and Oituz, representing a turning point in the war on the Eastern front (*Romania during First World War*, 1987, vol. 2, pp. 832-833).

In the 1917 reorganization process, Romanian soldiers and officers were trained in new intelligence skills developed on the Western Front, as stressed the provisions of a new normative document from January 20, 1918: *Instructions on the duties of the various echelons of Intelligence Service* (Spânu, 2012, pp. 256-266). The document provided the information requirements, the intelligence means and personnel. Thus, everyday combat operations at every echelon, especially by infantry and artillery elements, led to intelligence collection opportunities.

Each combat unit had its own information office and procedures requiring collection and dissemination of information within its sector, by intelligence officers and special agents. They conducted screenings, interrogations, and debriefings of civilians on the battlefield, prisoners of war and detainees to collect information, and drafted intelligence reports. All reports generated by daily operations supplemented other material including aerial photography and patrols observation. According to Terrence J. Finnegan, the most voluminous source of intelligence information in positional war came from the interrogation of prisoners. (Finnegan, 2009, pp. 29-30) In the Great War, the capture and retention of prisoners took place during all levels of operations on both sides. Not only was a captive one less

threat, prisoners were often treasure troves of information on critical issues that other forms of collection threw no light on.

Source: https://romaniadacia.wordpress.com/2014/11/16/for-the-heroes

Concerning the prisoner interrogations, the document state that: "Interrogation of a deserter or prisoner will give good results if executed by officer informant from Regiment even in an observer or trenches so that the prisoner can show on the ground the points on which he make declarations" (Spânu, 2012, pp. 253) It took great care in separating prisoners. Personal letters, documents, and correspondence taken from prisoners helped in identifying opposing units and provided information for tactical and strategic analysis. Interrogators used data from detailed photographic mosaics of his sector to trace with sources, prisoner or deserter, their itineraries from the rear to the front line trench network, confirming statements with specific details from photographs to include an isolated tree, house, or any other visible feature.

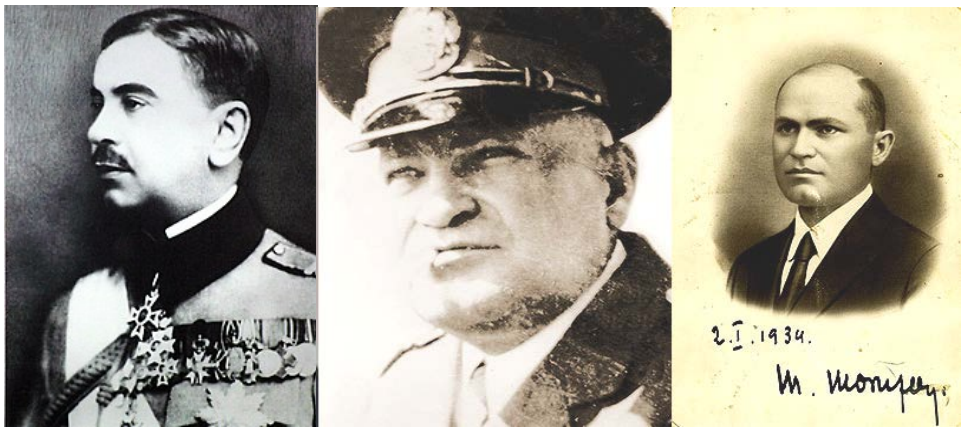
Human intelligence also came from the interrogation of repatriated civilians who crossed through Allied lines from German-held territory. Interviews were normally conducted by intelligence personnel in the sector in which they crossed to whatever information the refugees had on nearby German activity and intentions. Today this are the features of an HUMINT collector job.

The information offices also had a counterintelligence component where intelligence agents were instructed to look for the antennae of enemy listening devices. At the same time the Information Office had a Secret Service which was appointed with a military officers as head of the Service, a police officers and a number of secret agents for espionage and counterespionage activities.

A permanent intelligence service with specialized elements: from agents to HUMINT collectors

After the 1917 campaign, the head of the Information Office within the Romanian Army's the General Headquarters realized the necessity for some sort of permanent intelligence service. Thus, in the Report no. 289 from April 28, 1918, Col. Nicolae Condeescu, the Head of the Information Office, proposed the organizing principles of a permanent intelligence structure after the demobilization from July 1st, 1918 (Spânu, 2012, pp. 267-269), proposal approved in May by General Christescu. The document prove the military leaders' interest to keep the Information Office organization and functioning: two offices and the Secret Service appointed with special intelligence agents for espionage and counterespionage activities.

Until 1927, Army's the Secret Service, which was the core of the Romanian Intelligence Service from interwar period, was organized and reorganized several times however keeping its mission: collecting intelligence by using nonofficial covers or secret agents permanent employees of the Secret Service, and trained personnel to centralize and exploit information gathered



Col. Nicolae Condeescu and Mihail Moruzov.
Source: https://ro.wikipedia.org/wiki/Nicolae_Condeescu and
https://commons.wikimedia.org/wiki/File:Mihail_Moruzov.jpg

A special moment was the 1924 year when at the head of the Secret Service was appointed Mihail Moruzov. During the entire time he ran the Secret Service, Mihail Moruzov strived to introduce modern principles for conducting the intelligence activity. For this, he emphasized the need for a modern recruitment policy, which principles reflect in the future organization

instructions. Specialized military and civilian personnel which can be characterized as HUMINT collector was targeted.

The Secret Service was reorganized through the *Provisional Instructions on Intelligence* (1927) – 6 sections were established – and specialized military and civilian personnel was employed. The objectives of the Secret Service were stated in article 42: "the Secret Service gathers, sometimes, accurate intelligence of vital importance for conducting operations, and this is often mixed with false information. Using it requires precision and an in-depth verification of sources" (Spânu, 2010, pp. 136-137).

The new context also allowed the elaboration of working norms aiming first and foremost to strengthen the counterintelligence capabilities. Consequently, inside the Secret Service was elaborated a set of documents entitled *Measures to insure that the enemy's intelligence activities carried out through spies do not succeed* (Spânu, 2010, p. 137), which set out the main lines of action or Service's requirements: 1) rigorously controlling both the foreigners who live inside the country and those who want to enter it; 2) surveillance of suspected military and civilian individuals; 3) surveillance of the meetings between intelligence and army officers and foreigners, as well as the surveillance of individuals who move around commandments, military barracks and troops while conducting military exercises; 4) establishing permanent duty posts within the army and commandments so as to make impossible intelligence collection; 5) instructing military personnel, of all ranks on the negative actions of enemy espionage agents and the consequences of those actions for our army and means of defense; 6) raising public awareness and educating the society on the dangers posed by the subversive actions of the enemy through the publishing of literary works, based on real events.

These types of actions were assigned to counterintelligence agents, defined as "any individual who contributes in peace and war time to the deterrence of enemy actions conducted with covert means, in order to determine the defense capacities of the opponent's army" (Spânu, 2010, p. 137). In addition, the Secret Service adopted complex instructions regarding the manner to set up surveillance operations of suspicious persons, where there are mentions of the qualities required of agents and the manner in which missions should be executed: "Agents must have the following qualities: moral loyalty; firm beliefs, should lack inclinations towards drunkenness or other vices, should possess courage, agility, presence of spirit, be physically fit, be persistent, cautious, fellowship, take a responsible and serious attitude towards their work responsibilities, as well as towards the entire state security system, strong body, strong legs, good sight, hearing and memory as well as a common appearance" (Spânu, 2010, p. 137).

M**ultiplying the number of specialized elements**. The document we are going to refer to in the next section was preserved in the archives under the name of *Statute of the S. Service*, and entered into force, as it is mentioned in article 12, on April 20, 1934 (Spânu, 2010, pp. 240-245; Troncota, 2008, p. 147). It is about the increasing role and importance of the Secret Service of Information although it stays within the military intelligence structure.

According to article 1: "The S. Service is the technical body of the Army's Intelligence Service (Spânu, 2010, pp. 240-245). Article 5 was very important because it established for the Secret Service the task of recruiting and training capable elements of executing intelligence missions, domestically and abroad, according to the requirements of the Service, the documents provide information about military and civilian elements used as three category of agents who had to be trained inside the Service were functioned a special training program: indicating agents, recruiters and contact agents. As the document state, the human resource was a permanent concern for the Secret Service. This is why article 6 regulated the manner in which personnel appointments and promotions were to be made. Secret Service could formulate proposals for the appointment of government officials and directly appointed its own covert personnel, according to the Service's needs. The appointment decisions as well as the persons' files were kept in its own archive. The overt personnel were appointed through a ministerial decision, while the covert personnel could not be appointed or replaced, by anyone but the Secret Service (Troncota, 2008, p. 147). Moving a person from the category of covert personnel to overt personnel could be made only on the basis of a report, addressed to the Defense Minister, who could decide in favor of moving that person in the ranks of the overt personnel, situation in which the real name of the employee was introduced in the payments sheet. Moreover, the entire personnel of the Secret Service was considered to be a "specialized element" (Troncota, 2008, p. 147).There is a similarity with the activities carried out in the HUMINT spectrum which can be covered and uncovered.

The Secret Service organization and functioning instruction were not changed but threats multiplying in relation to new domestic and international political context. Therefore information requirements multiplied and consequently the number of agents multiplied. Through order no. 668 from January 1st, 1938, the Secret Service passed from the Ministry of Defense under the authority of the General Staff of the Army.

Consequently, a new document, classified "Top Secret" was adopted entitled *Ministerial Decision no 2.200 from March 29, 1938 regarding the organization of the "S" Service of the General Staff of the Army and the justification of the intelligence fund.* (Spânu, 2010, p. 335) This document

emphasized the need to adapt the Secret Service in order to be able to respond to wartime intelligence needs: "The Chief of Staff [...] will give all the orders and instructions necessary for the organization and functioning of the S. Service so that it can respond in time of war to the operational needs of the army" (Spânu, 2010, p. 335).

The norms regarding the appointment of the personnel were almost entirely preserved during the 1938 reorganization (Spânu, 2010, p.253). However the number of the Service's personnel, civil and military, reached in 1939 to 36 officers and 306 civilians including 44 principal agents and 100 special agents. It was about the agents which was trained for intelligence missions, domestically and abroad, according to the requirements of the Service. At the same time, it was about civilian personal specialized in intelligence analysis, which was aimed at deepening understanding of tactical and strategic situations, including events in progress. In 1938 the Service needed information on military and political evolutions both from Western and Eastern Romanian boarders.

Conclusions

For the large public, collection of information/intelligence from human sources (HUMINT), the oldest of the existing methods, identifies itself with spying and clandestine activity. Consequently, there is a similarity between the terms used to designate the person providing the information, agent, source, informant, collaborator, which we emphasized in this study. For the purpose of our research, we used the term agent to refer to the person being recruited and employed by the Intelligence structure to obtain secrets or carry out covert activities. After a short presentation of the changes occurred in intelligence field during the Great War, we examined the Romanian Interwar period Secret Service archival documents in order to identify which was the recruitment policy and what were the characteristics of intelligence agents and if there is a similarity with the characteristics of the HUMINT collector.

In the Great War, unfortunately, the lack of organization of an intelligence structure within Romanian Army was reflected in the defeat suffered in the first part of the Romanian campaign. However, after the great defeat from 1916, Romania embarked on the reconstruction and strengthening of its combat capability during the first half of 1917 through multiple national efforts and with the French Military Mission contribution. In terms of intelligence, the French mission provided the equipment and technical support the Romanian army needed. The Romanian expertise acquired during the First World War highlighted the close link between

human resource, armament and combat equipment. However, it is operational and tactical intelligence, not necessarily numbers, technology, or tactics that can have the most decisive impact on how forces are employed and how success is achieved in wartime operations.

Concerning the professionalization of the information agents, the archival documents provide information about the prisoners or deserters interrogations as a principal mean to collect information about enemy: *interrogations to be made only by intelligence officers and translators from intelligence offices of every army unit*. Thus, we can recognize some of the HUMINT collector characteristics, both offensive and defensive activities, especially when it comes to the activity of military units. In offensive actions, collecting information from human sources provides information on the environment of operations (geographical, social, political), establishing relations with civilian or local people in an area, detecting enemy positions, and providing the elements necessary for establishing the details of offensive missions. In terms of defensive activity, HUMINT collectors aim to detect the intentions of the enemy forces about the risk of an attack and to ensure that their forces are mobilized for a counter-attack, or for a position that allows for minimal loss of human resources, or materials.

For the interwar period, the existence of documents which regulate the activity of the Secret Service *shows the permanent concern of the Service's leadership to recruit and train the human resources*. Secret Service could formulate proposals for the appointment of government officials and directly appointed its own covert personnel, secret agents, according to the Service's needs. The professional training of the personnel, irrespective of the compartment in which they were operating represented the responsibility of each manager. Another permanent concern for the Service's leadership in addition to training the human resources was insuring its counterintelligence protection. Thus, censorship was imposed to curtail any chance of an enemy acquiring a critical snippet of information. This was achieved by hiding the identity of the employees. Each member of the Service used for the transmission of information a numerical code, and he communicated only with this direct hierarchical superior. During the entire interwar period, Mihail Moruzov strived to introduce modern principles for conducting the intelligence activity. For this, he emphasized the need for a modern recruitment policy, which principles reflect in the future organization instructions. Specialized military and civilian personnel, which can be characterized as HUMINT collector, was targeted.

References:

1. *Air Force Pamphlet 200-18, Target Intelligence Handbook: Unclassified Targeting Principles*, Washington DC: Department of the Air Force, October 1, 1990. Available on-line on http://fas.org/irp/nsa/ioss/threat96/part02.htm.

2. Finnegan, Terrence J., Col., USAFR (Ret.), *The Origins of Modern Intelligence, Surveillance, and Reconnaissance. Military Intelligence at the Front, 1914–18,* in *Studies in Intelligence*, Vol. 53, No. 4 (December 2009), pp. 25-40, available on-line on https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no4/military-intelligence-at-the-front-1914201318.html

3. *Human Intelligence Collector Operation. Field Manual Headquarters No. 2-22.3*, Department of the Army Washington DC, 6 September 2006, available on-line on https://fas.org/irp/doddir/army/fm2-22-3.pdf

4. *Language of espionage*, available on-line on http://www.spymuseum.org/education-programs/news-books-briefings/language-of-espionage.

5. *Legenda unui General (The Legend of a General)*, by Stelian Tănase, 7 December, 2015, available on-line on http://www.stelian-tanase.ro/legenda-unui-general/

6. Lerner, Adrienne Wilmoth, *World War I. Encyclopedia of Espionage, Intelligence, and Security* available on-line on http://www.faqs.org/espionage/Vo-Z/World-War-I.html.

7. Otu, Petre, (coord.), *Reforma militară și societatea în România, de la Carol I la a doua conflagrație mondială*, Occasional papers, Year 6, no. 8, 2007.

8. *România în anii primului război mondial* (*Romania during the years of World War I*), 1987, Bucharest: Military Publishing House, vol. 2.

9. Spânu, Alin, (2010), *Istoria serviciilor de Informații/contrainformații românești în perioada 1919-1945*, Iași: Demiurg Publishing House.

10. Spânu, Alin, (2012), *Serviciul de Informații al României în războiul de întregire națională (1916-1920)*, Bucharest: Military Publishing House.

11. Suvorov, Victor, (1984), *Inside Soviet Military Intelligence*, Chapter3, Agents, MacMillan Publishing Company, available on-line onhttp://militera.lib.ru/research/suvorov8/16.html and http://en.academic.ru/dic.nsf/enwiki/ 8238028#cite_note-Suvorov-IM-03-0.

12. *The Stratford Glossary of Useful, Baffling and Strange Intelligence Terms,* available on-line on http://www.scribd.com/doc/219780109/The-Stratfor-Glossary-of-Useful-Baffling-and-Strange-Intelligence-Terms#scribd

13. Troncotă,Cristian, (2008), *România și frontul secret 1859-1945 (Romania and the Secret Front)*, Bucharest: Elion Publishing House.

14. *U.S. Army Human Intelligence Collector Field Manual*, Department of the Army, Rowman & Littlefield, 6 January 2015, available on-line on https://books.google.ro/books?isbn=1493016229

THE RELATIONS OF THE SECURITATE WITH SIMILAR STRUCTURES OF THE MEMBER STATES OF THE WARSAW TREATY ORGANIZATION. FROM INFORMATION EXCHANGES TO ISOLATION

Mircea STAN *

Abstract

This article attempts to present a perspective on the collaboration of Romanian security and information services with similar structures in the Warsaw Treaty Organization countries during the Cold War.

The assumptions made by the article are: the absence of a study exclusively dedicated to the problem; the possibility of researching documents from physical or virtual archives recently declassified and given for research; the importance of exchanges of information in the work of Cold War security and intelligence services; Romania's effectiveness in exchanging information with partner countries and the impact on national security; the inefficiency of the inter-institutional collaboration between the Romanian intelligence and security services with similar structures due to the political oscillations in Bucharest.

From the analysis of the available scientific material, exchanges of information between the Securitate and the homologous services of the Warsaw Treaty Organization experienced oscillating periods, from constant information exchanges to some sporadic ones, and by the end of the Cold War these exchanges did not exist. Lack of institutional collaboration was a factor for which the Securitate was de-institutionalized as an institution in December 1989, influencing Romania's evolution as a state on the international stage.

The dissolution of security and intelligence services at key moments of a state's history is not a desirable scenery for the security of that state, in my opinion this is rather the biggest vulnerability of that state.

Keywords*: security*, *intelligence*, *counterintelligence*, *espionage*, *intelligence cooperation*, *diplomacy*

The study aims to demonstrate whether there was collaboration and how effective this collaboration was, between the Department of State

* PhD student „Mihai Viteazul" National Intelligence Academy,stanmircea90@gmail.com

Securitate and similar structures within the Warsaw Treaty Organization (WTO), and if this had a direct impact both on the evolution of the Romanian security and intelligence services, as well as Romania's evolution on an international level after 1989. For a small state such as Romania it was impossible to provide itself with the necessary intelligence regarding a sustainable development. Exchanges of bi- and multilateral information between the Romanian security and intelligence services with similar structures in the WTO countries have existed but will diminish considerably towards the end of the Cold War. The Department of State Security found itself isolated near and during the events of December 1989, which in my view contributed to the destruction of the security institution and the state.

Inter-Agency Intelligence has been imposed as a necessity of intelligence gathering since the emergence of the first institutionalized intelligence/counterintelligence structures. The fall of the Iron Curtain across Europe triggered a "race" between the secret services on one side and the other during the Cold War. Just as the popular democracy regimes were installed in the Central and Eastern European countries through coercive means and with the help of the Soviets, the security and intelligence services of these regimes were created under close supervision and Soviet model. The new geopolitical configuration and the imperialist threat required a "fraternal" collaboration of intelligence /counterintelligence structures in the socialist countries. The issue of studying such collaboration is diminished by the lack of material on the specificity of the problem and the course followed by certain archives after the collapse of communist regimes. Romania’s situation is special in this issue due to the fact that the country was enrolled on its own trajectory targeting a foreign policy line and a security agenda independent of the directives drafted by USSR in the other countries in its sphere of influence.

A careful analysis of the available information highlights that for the duration of the existence of the Securitate as a law-based institution, its relations with security and intelligence services in the socialist camp have seen growth and decline. Overall, it may be admitted that there was an ineffectiveness of Securitate's co-operation with homologous services largely due to divergences in political evolution. In the case of Romania, the interinstitutional collaboration or inter-agency intelligence, according to current usage, can be phased in as follows: a) a stage in which in each socialist country the activity of intelligence/counterintelligence was led by the Soviet counsellors and attempted a close collaboration with KGB (Komitet Gosudarstvennoi Bezopasnosti - State Security Committee of the USSR, 1954-1991) - GRU (Glavnoe Razvedîvatelnoe Upravlenie - the Soviet military

espionage service or the Military Intelligence Directorate), as authorities in the field; b) a second stage, after the declaration of the "Brezhnev Doctrine", attempting to reset the interinstitutional collaborations of the system, in which USSR hoped that Romania would return to its original boldness; c) the last step is identified with the loss of patience of the former partners to wait for the Romanian state to return to its initial position. In fact, the last step finds Securitate in total isolation from similar services and labelled as enemy of the latter.

Sending Soviet advisers to all communist countries to help reinforce the regimes tends to support the idea that there have been bilateral or multilateral meetings on the secret services line since 1947-1948. The idea can be denied on the basis of current information. KGB would not have wanted multilateral contacts between the secret services in the fraternal states because it would have made it harder for its missions to obtain the information it wanted from each country. A first step towards bilateral co-operation was reached in 1950, between MGB (Ministerstvo Gosudarstvennoy Bezopasnosti - Ministry of State Security of the USSR in the period 1946-1953) and ÁVH (Államvédelmi Hatóság - Hungarian State Security, 1948-1956) through the espionage departments at the initiative of MGB. It was intended to coordinate projects and activities, controlled by the Soviets, led by Colonel Filatov first, then by the Colonels Tikov and Jelisejev, against SFRY (Socialist Federal Republic of Yugoslavia)[1].

Such collaborations varied from one state to another. The most obedient services to KGB were KDS (Komitet za dăržavna sigurnost - Bulgarian State Security), STASI (Das Ministerium für Staatssicherheit - Ministry of State Security or East-German State Security, 1950-1990), StB (State Security - Czechoslovak State Security), ÁVH, SB (Służba Bezpieczeństwa - Polish State Security), at the other end of the line being located (Department of State Securitate). The Bulgarian KDS was so dependent on KGB that on a visit from May 27 to June 1, 1968, for an exchange of experience with SCC (State Security Council of Romania, 1968-1967) Lieutenant General Mircio Spasov would say that:

> *"USSR is the one that gives confidence in defending the security of the socialist countries and that without USSR our countries could not*

[1] László Ritter, „The Soviet – Hungarian Intelligence Co-operation in the Early Cold War Period" in *NKVD/KGB Activities and its Cooperation with other Secret Services in Central and Eastern Europe 1945-1989*, Alexandra Grúňvá (ed.), Bratislava, 14-16th November 2007, p. 248.

do much. As for Bulgaria and its security authorities, it could not even conceive of existence without the support of USSR"[2].

The first multilateral meeting, evidenced by documents, of representatives of the secret services in the communist sphere took place in 1955, in the context of the foundation of WTO (May 14, 1955). The data on such contacts are incomplete, so the first meeting would take place in Bucharest, being seconded by two other in Berlin and Prague[3]. The Prague meeting would lay the foundations of the "Radio Counter Intelligence Coordination Group", which was set up in Warsaw in 1956. They attempted jamming the entire electromagnetic spectrum, especially the R.E.L. (Radio Free Europe), whose activity was considered a threat to communist regimes[4].

There have been several attempts to collaborate on intelligence and technology exchanges. Between 4 and 6 March 1958 a meeting was held in Bucharest between representatives of PRR (People's Republic of Romania), USSR, PRB (People's Republic of Bulgaria), HPR (Hungarian People's Republic), CSR (Czechoslovak Socialist Republic), focused on: fighting subversive actions orchestrated by Western espionage; improving the exchange of information and conducting joint actions[5]. Just one year after this multilateral meeting was also held in Bucharest, between 4 and 12 March 1959, a meeting between the Romanian and Bulgarian delegations to coordinate the activities regarding the identification of the Romanian royal intelligence agency that had activated against Bulgaria and other issues of common interest[6]. It should be noted that throughout the sixth decade KGB had a real "tournament" of bilateral contacts with the similar secret services in the communist states, most of the contacts being established with the StB. Also during the year 1958 there were exchanges and requests for information between the Securitate and similar Hungarian, Bulgarian and Soviet services[7].

---

[2] The Archives of the National Council for the Study of the Securitate Archives (A.N.C.S.S.A.), Documentary Fund, File No 88, vol. 4, tab 288.

[3] Florian Banu, „From collaboration to isolation. The relations between the Securitate with similar service of intelligence of the Warsaw Treaty Organization, 1955-1989, part I", in *Archives of Totalitarism*, Year XXIII, No 86-87, 1-2/2015, p. 127.

[4] *Ibidem*, p. 127.

[5] Bulgarian Archive of the Ministry of the Interior, Sofia, Fond 2, Record 1, File N0 1345, „Report from Gen. M. Spasov on Multilateral Security Meeting in Bucharest", March 12, 1958, in *C.W.I.H.P.* (Cold War International History Project).

[6] Bulgarian Archive of the Ministry of the Interior, Sofia, Fond 2, Record 1, File N0 1339, „Report on Visit to Romania on Counterintelligence Issues", March 23, 1959, in *C.W.I.H.P.*

[7] Romanian Intelligence Service, *The White Book of the Securitate*, vol. III, doc. No 13, 16, 18, Bucharest, 1995, pp. 154-156.

After escalating tensions between Romania and the USSR as a result of the assassination attempts on Dej[8], a program of massive security and military cleansing has been initiated, which will be more intense after 1961. Year 1961 was the last time the Securitate sent personnel to study in the USSR, until then the training courses followed by future Romanian officers at the Felix Djerjinski Institute of the KGB being of notoriety.

A document attesting the escalation of disagreement between the Securitate and the KGB is the discussion between Alexandru Draghici and Piotr Ivanovici Ivaşiutin, the deputy of the KGB president. On P.I. Ivaşiutin's statements insisting on a better collaboration between the Securitate and the KGB against the espionage conducted by the adversary block, based on the agreement between the Romanian side and the Soviet side, by the voice of Vladimir Efimovici Semiciastnii (KGB president 1961-1967), A. Draghici felt the need to intercede and say that the relation between the two institutions is strong, specifying that "the materials we send to you daily and our work prove it." The same Draghici firmly affirms that he disagrees with the inequality between the institutions, given the willingness of KGB to know in detail the Romanian agentura. As a reply, Ivaşiutin stated:

> *"See, Comrade Draghici, for so long I told Zaharovski: what do you need for the conspiratorial names of the friendly countries' agents? How important is the information coming from Popescu or other names of your agents? Is not it enough that it comes from the RPR Ministry of the Interior? He did not want to listen to me. That does not mean we have evidence of your agents. We do not have this, and I would propose that a delegation from you come to us and to check each case individually".*

The same document presents Draghici's disagreements with the large number of Soviet officers maintained by USSR in the vicinity of the Romanian State apparatus, since they were no longer useful and when consulted on certain issues their only answer was "vaşii delo"[9].

---

[8] Larry L. Watts, *With Friends Like These...The Soviet Bloc's Clandestine War Against Romania*, english translation by Camelia Diaconescu, Bucharest, RAO Publishing House, 2011, p. 33, 235, 511.

[9] National Central Historical Archives (N.C.H.A.), Central Committee of Romanian Comunist Party Fund (C.C. of R.C.P.), Administrative-Political Section, File Nº 13/1962, tabs 2-6. See also: National Council for the Study of the Securitate Archives (N.C.S.S.A.), *The Party and the Securitate. The history of a failder idle (1948-1989)*, doc. Nº 91, Bucharest, Florian and Luminita Banu (eds.), Iasi, Editorial Demiur House, 2013, pp. 351-355.

The conflicts between the Romanian and the Soviet side became more acute in 1962, when Dej and Alexandru Drăghici made the decision to create a "small group of officers", a "core" of counterintelligence and counterespionage officers to deal with "The identification of the Soviet agentura in Romania"[10]. The idea of creating this group to deal with the Soviet agents in Romania had been put into practice in a sensible way after the withdrawal of Soviet troops from Romania. The work of this team was perfectly conspicuous, not even the Department of Counterintelligence within the Securitate knew of its existence[11].

As mentioned above, Romania could not have supported its security and intelligence agenda if Moscow had not been involved in extra-block events, in this case the Cuban Missile Crisis. The issue of recruitments made by PGU (Pervo Glavnoe Upravlenie, Central Directorate I - Foreign Intelligence, Soviet Espionage, 1954-1991) and GRU on the territory of Romania was brought to the discussion between Dej, Bodnaras and Ceausescu, on the one hand, and Khrushchev, on the other hand, following the visit made by the latter to Romania in 1962. Following this episode, Khrushchev ordered the other security and intelligence services from the Soviet block to limit their cooperation with similar structures in the RPR to exchanges of general, itemized information that would not be in the benefit the Romanian state[12]. Dej's reaction was almost immediate and consisted in the formalization of the counterintelligence "core" within the Counter Intelligence Directorate, expanding its activity against all agenturas of the socialist countries[13]. Subsequently, this group of counterintelligence officers will form the future MU (Military Unit) 0110[14].

On May 13, 1963, Dej made the decision to answer Vladimir Efimovici Semiciastnii (KGB director 1961-1967) following the 1962 warning of the latter, motivating to the KGB director that:

> *"given the current circumstances, the maintenance of the two councillors in the service of the Ministry of Interior is no longer necessary and that, in the future, cooperation between the two ministries will take place only at the highest level"[15].*

---

[10] Cristian Troncota, *The Duplicitous: a history of security and intelligence services of the communist regime in Romania: 1965-1989*, second edition revised and added, Bucharest, Elion Publishing House, 2014, p. 25
[11] *Ibidem*, pp. 25-26; Larry L. Watts, *op. cit.,* 216.
[12] Ladislav Bittman, *The Deception Game: Czechoslovak Intelligence in Soviet Political Warfare*, Siracusa, Syracuse University Research Corporation, 1972, p. 146.
[13] Cristian Troncota, *op. cit*, pp. 26-27; Larry L. Watts, *op. cit.,* pp. 218-219.
[14] Between 1969-1978 it was named M.U. 0920/A, then from 1978 to 1989 M.U. 0110. The M.U. was led by Aurel Mircea 1963-1965, Constantin Iosif 1965-1978, Victor Neculicioiu 1978-1989.
[15] N.C.H.A., C.C. of R.C.P. – Writing Section Fund, File Nº 10/1963.

After the "April Declaration of 1964", an accelerated dissemination of the document took place throughout the Romanian administration, with the obvious purpose of demonstrating that URSS had intervened strongly in the Romanian internal affairs. Massive purges of security, militia, and army personnel have been conducted, based in particular on ethnic and professional criteria. Drăghici ordered the heads of the central units of the Securitate to limit the flow of information to the Soviet councillors since 1962, thus removing them from the informative activity.

The arrival of Leonid Ilici Brezhnev as Secretary General of CC of PCUS (Central Committee of the Communist Party of the Soviet Union) on 14 October 1964 constituted an opportunity of which Dej took advantage of to request the withdrawal of the last Soviet advisers from Romania. After several exchanges of telegrams between the heads of the two homologous security and intelligence structures and after the unannounced visit of Semiciastnii and Saharovski in Bucharest (November 1964), it was concluded that USSR must withdraw its last advisers from Romania in December 1964[16].

The withdrawal of Soviet advisers on security and intelligence issues since 1958 and culminating in 1964 must be carefully considered. The political - strategic movements of Communist leaders are not entirely original, but they have changed the security architecture in Central and South - Eastern Europe. What's more, the question is why should the Soviets give up so easily to the Romanian counsellors? The answer may also come in the context in which, prior to the withdrawal, large spy networks had been created to form "underground" channels of communication with Moscow. Therefore, the phrase "we just left to stay" can be supported. Here are some other things to be mentioned at least: the Securitate's institution was gradually expelled from the transformation program of KGB initiated between 1962 and 1964 in the other Warsaw Treaty countries, and in 1965 Romania was left out of the war strategy of the Warsaw Pact[17].

Regarding Romania, although it did not recognize the creation of GDR (German Democratic Republic), the closest contacts during Dej's leadership were with STASI In addition to the kidnappings of Aurel Decei and Oliviu Beldeanu, the Securitate collaborated with STASI on several levels, from exchanges of information on Romanian refugees from the GFR (German Federal Republic) to information exchanges concerning the operative technique. Near the "Declaration of April 1964" there were two bilateral meetings between the leaders of the two security and intelligence institutions.

---

[16] Cristian Troncota, *op. cit*, pp. 33.
[17] Larry L. Watts, *op. cit.,* pp. 33-34.

Thus, in 1962, Erich Mielke[18], director of STASI, accompanied by Markus Wolf[19], the director HV A. (Hauptverwaltung A.-Aufklärung, East German Central «espionage» Administration) followed by a return visit by a delegation of DFI (Directorate for Foreign Intelligence, the correct name is Directorate A - External Intelligence or Directorate I, after reorganization, between 1951 and 1963) led by Nicolae Doicaru accompanied by the Director of the Department for Operational Techniques of the DSS in April 1963. Both visits were made on the background of the STASI's initiative to establish "ways of contacting other communist secret services, trying to identify forms of technical and operative collaboration"[20]. An indication of the high degree of collaboration between Securitate and STASI is revealed by the existence of the Securitate Task Force in East Berlin, whose members from 1950 to 1960 functioned as officials of the Embassy of Romania in East Berlin. Two things draw particular attention to the Security Task Force: 1) all actions were approved and supported (probably logistic n.r.) by STASI .; 2) the degree of collaboration was so great that the Task Force was named, according to the archives of STASI, the "Romanian Group" or "Romanian Friends"[21].

Information exchanges between the Securitate and similar structures in countries with the same political regime remained high until Dej decided PRR to follow another course on the evolution of the political system. The "New Policy" in Bucharest could not to affect the Securitate's cooperation relations. A series of events conducted by RWP (Romanian Workers' Party) have made the Securitate to be sidelined by "partner" services. Romania's opposition to WTO decisions coupled with a series of pro-Western diplomatic actions and the removal of the last Soviet councillors (December 1964) from the PRR have not been left unanswered. The exclusion of the Romanian state from the large socialist information community was made gradually, first on the order of Nikita Sergeyevich Khrushchev given to the socialist countries to limit their co-operation with Romania in the field of espionage, then to eliminate the Securitate from the coordinated program of active measures initiated in 1965 by the KGB from Lubianka[22].

After 1964, information exchanges will not disappear, but they will be more sporadic. After Romania's enrolment on a different line of foreign policy, the first exchange of information was between DSS and KDS Thus, on

---

[18] Erich Fritz Emil Mielke, chief of STASI between 1957-1989.
[19] Markus Johannes Wolf, chief of HV A. between 1953-1086.
[20] Stejarel Olaru, Georg Herbstritt, *Stasi and the Securitate*, Bucharest, Humanitas Publishing House, 2005, pp. 66-67.
[21] *Ibidem*, 288-289.
[22] Ladislav Bittman, *op. cit.,* pp. 144-146.

28 October 1965, an exchange of letters between the Ministers of Internal Affairs of the two countries, Cornel Onescu and Angel Solakov, provided information on the actions of OTAN on the European continent[23]. Then a request from Minister Solakov on certain Italian citizens was addressed on 9 January 1966 to Cornel Onescu[24].

Moscow order on restricting information sharing with R.S.R. is also revealed by a report of the KGB in 1967. The document mentions the low degree of cooperation with the Romanian Security, limited to minor exchanges of information. Romania was so marginalized that the Soviets preferred to re-establish contacts with the State Security Ministry of DPRK (Democratic People's Republic of Korea)[25].

The arrival of Nicolae Ceausescu at the head of RCP (Romanian Communist Party, 1965-1989) meant a continuation of the foreign policy started by Gheorghe Gheorghiu - Dej. The way of national communism chosen by SRR (Socialist Republic of Romania, 1965-1989) culminated with Ceausescu's intervention to condemn the invasion of WTO troops led by USSR in CSR. Once this moment passed, the situation inside the communist block against the unaligned position of the Romanian state has been relieved. The framework for the resumption of some forms of bilateral cooperation between the Securitate and the homologous services of the Warsaw Pact has been created. The year 1968 constituted a moment of profound reformation of the Securitate, with extensive transformations taking place inside the institution. The most significant aspect is highlighted by the reduction of the informational network (including informants, collaborators, residents, meeting host houses and conspirators) from a total of 118,952 on January 1, 1968 to 85,042 on December 20, 1968[26].

The movement of troops on Romania's borders after the invasion of Czechoslovakia and the enunciation of the "Brezhnev Doctrine" led Ceausescu to take preventive measures to defend the country. One of these measures consisted in the resumption of sensitive relations with former secret services. The last multilateral meeting on security and intelligence matters took place between December 8 and 11, 1970 in Budapest, on external intelligence

---

[23] Bulgarian Archive of the Ministry of the Interior, Sofia, Fond 1, Record 10, File N^0 338, „Correspondence between Gen. A. Solakov and Gen. K. Onescu on Acquired Intelligence Information", December 22, 1965, in *C.W.I.H.P.*

[24] Bulgarian Archive of the Ministry of the Interior, Sofia, Fond 1, Record 10, File N^0 338, „Letter from Gen. A. Solakov to Gen. K. Onescu on Information on Italian Citizens", January 09, 1966, in *C.W.I.H.P.*

[25] TsKhSD, f. 89, op. 5, d. 3., II, 1-14, „The KGB's 1967 Annual", May 06 1968, in *C.W.I.H.P.*

[26] A.N.C.S.S.A., Documentary Fund, File N^o 88, vol. 3, tabs 13-14.

matters[27]. During the meeting a number of issues were discussed, among which the most important ones were: the need to create a unique centre where data about the personnel, the agentura and the legends used by the adversary services should be available; linking partner countries' foreign residences in order to obtain a fast management of operational problems; creating a single coordination centre for setting out the main directives for achieving common objectives[28]. Other documents related to the multilateral meetings in which our country took part do not result from uncovering the archive documents.

At bilateral level, the best cooperation of the Securitate was with STASI, diminished considerably after 1973. A remarkable episode happened on March 18, 1971, when, contrary to all protocol matters, Nicolae Doicaru, arriving from Copenhagen, made a stopover in East Berlin where he had a meeting with Erich Mielke[29]. The conversation between Doicaru, head of Romanian espionage and his counterpart, Markus Wolf, highlights the ridiculous situation created by Doicaru himself in the failed attempt to regulate the forms of bilateral collaboration between the two external intelligence services.

During this time KGB concluded collaboration protocols with all the other socialist services except SRR, reaching the point where, through a collaboration protocol dated December 6, 1973, the KGB would be allowed to recruit East German nationals for fulfilling the missions, situation in which STASI had to provide ongoing contacts[30].

There was a "friendship group" within the socialist camp with which Moscow has developed much closer relations based on the unconditional submission of Communist leaders of those countries to Moscow. GDR, CSR, HPR, PRB, PPR (Polish People's Republic) "benefited" from a positive image in front of the Kremlin, in contrast to SFRY, PRA (People's Republic of Albania) and SRR. The actions of KGB at regional or international level against specific objectives benefited from the broad support of intelligence services of WTO member countries. As the relationship between SRR and the other WTO

---

[27] Florian Banu, *op. cit.,* p. 74. According to other sources, HV A. has bilateral cooperations relations with all WTO counterpart services and at the multilateral level at a four years interval, the last such meeting took place in East Berlin in 1988. Romania was not invited at that meeting instead Cuba was. See also: Paul Mandrell, „Cooperation between HV A. and the KGB, 1951-1989", in *German Historical Institute Bulletin,* Richard F. Wetzell (ed.), Supplement 9 (2014), p. 173.
[28] A.N.C.S.S.A., Documentary Fund, File Nº 16124, vol. 7, tabs 196-197.
[29] Stajarel Olaru, Georg Herbstritt, *op. cit.,* doc. nr. 7, pp. 288-299.
[30] BStU, MfS, ZAIG 13.730, pp. 1-15, „Agreement on Cooperation between the Stasi and the KGB, 6 December 1973", December 06, 1973, in *C.W.I.H.P.*

member states deteriorated, KGB took the decision to coordinate a program of anti-Romanian active measures, largely based on disinformation. Among the informative adversaries who have acted against the Romanian state, the best known are KGB, ÁVO/ Hungarian[31] ÁVH and STASI through HVA due to their representativeness through the Hungarian and German communities in our country, used as a front for their operations[32].

Romania's relationship with other WTO member states has constantly deteriorated since 1965. The incontinence of Moscow's orchestrated actions against the Romanian state materialized, first of all, in the program of active measures. These were focused on two aspects: on the one hand, they aimed to isolate Romania internationally and to create the image of "Soviet Trojan horse" in the West and in the Third World countries, and on the other hand it was hoped to create dissension between the members at the top of power[33]. Besides these aspects, some states had independent reasons to act in Romania. Alongside Bulgaria and Hungary who had territorial claims, GDR conducted hostile actions against the Romanian state because the Bucharest authorities refused to recognize the breakup of Germany. The ruling circles in Bucharest had concluded, through secret negotiations, a treaty with GFR[34].

The bilateral relations between SRR and USSR worsened even further after the defection of General Ion Mihai Pacepa (July 1978). In the late 1970s USSR made the decision that PGU to transfer Romania from Department XI - "Links with the Socialist Countries" to Department V (dealing with some NATO member countries, Switzerland and the other two "rebel" states of the Soviet Block, Yugoslavia and Albania)[35]. There is no information to confirm whether at Moscow's order or not, but also the other Warsaw Pact partner countries have taken similar actions against Romania. Archival documents, for example, show that HVA transferred Romania among the countries belonging to Group C alongside the same Yugoslavia, Albania and distinctly from PGU, China[36].

During the 1970s, the relationship between DSS and KGB remained at an almost constant level. Although the Romanian side did not share the same visions with the Soviet leadership, the Romanian political squad eschewed a

---

31 After the Revolution of 1956, the institution of Security was abolished by János Kádár, Hungary become the only state member of the W.T.O. who did not have intelligence services, this structure's skills being passed under the Hungarian Ministry of Interior.
32 Larry L. Watts, *op. cit.,* p. 314.
33 Christopher Andrew, Vasili Mitrokhin, *The World Was Going Our Way: The KGB and the Battle for the Third World*, New York, Basic Books, 2005, p. 290.
34 Stajarel Olaru, Georg Herbstritt, *op. cit.,* pp. 80-81.
35 Christopher Andrew, Vasili Mitrokhin, *op. cit.,* p. 500.
36 Stajarel Olaru, Georg Herbstritt, *op. cit.,* 102.

free escalation of tensions with the USSR. Until 1975 DSS has collaborated with KGB in order to unmask and compromise Richard Wurmbrand, a character conducting a campaign of ideological diversion against the socialist countries and, in particular, against USSR[37]. Then there was an exchange of information in the "Usatiuc" and "Covalciuc" cases, to which two exchanges of information were added by the transfer of two sets of 12 documents each sent by KGB to DSS, the first on some aspects of the political-military evolution in America, Asia and Africa, and the second, dated March 3, 1972, including information on European countries[38].

SRR continued to conduct some forms of collaboration with other socialist countries in a reduced pattern. For example, on August 20, 1974, a "Convention between the Government of the Czechoslovak Socialist Republic and the Government of the Socialist Republic of Romania on Governmental Telegraphic and Telephony Encrypted Communications" and an additional protocol "Instructions for technical maintenance and exploit of the governmental telegraphic link between Prague and Bucharest" were concluded[39].

There were small and intermittent exchanges of information with PPR and HPR, cantered on support for informative-operative pursuit of some people, exchange of information on some countries in the adversary camp and mutual transfer of operative technique[40].

Since 1975, there has been a shift in security and intelligence cooperation between SRR and all the other "fraternal" states. Distancing occurred especially after the signing of the Final Act of CSCE (Conference on Security and Co-operation in Europe) on August 1, 1975, when Romania's role was visibly diminished throughout the process of the Conference through the concerted active measures conducted by Moscow. In a KGB report about the new directions of US policy regarding the European socialist countries it is

---

[37] Florian Banu, „From collaboration to isolation. The relations between the Securitate with similar service of intelligence of the Warsaw Treaty Organization, 1955-1989, part I", in *Archives of Totalitarism*, Year XXIII, Nº 88-89, 3-4/2015, part II, pp. 80-83.

[38] A.N.C.S.S.A., Documentary Fund, File Nº 13134, vol. 28, tab 166, 201.

[39] The Institute for the Study of Totalitarian Regimes of the Czech Republic, *Cooperation in the Eastern Bloc 1948-1989: documents on bilateral cooperation,* declassified 01.01.2008. Within this project a range of electronic documents are available on collaboration between socialist countries' intelligence services. Information exchanges and cooperation between CSR and SRR are reduced to only two documents, unlike the collaboration with GDR, where 102 documents are available. Within the same project in the section dedicated to "International Cooperation in 1989", CSR had collaboration protocols with all services in the Eastern Bloc, especially with KGB., except for the SRR Securitate.

[40] Florian Banu, *op. cit.,* part. II, 84-86.

shown that Romania continued to be a source of concern for Moscow because of the contrary positions within WTO and the independent foreign policy line. The same documents mention that Vice President George W. Bush's visit to Romania has strengthened Romania's sense of independence and strengthened the personal authority of Nicolae Ceausescu[41].

During the year 1976 there were exchanges of operative information with HPR regarding the West German citizen Rott Risard and the Polish citizen Rott Honorata. The request came from the SB through a telegram issued on March 4, 1976, requiring the informative - operative supervision of the two[42]. Towards the end of 1976, a delegation of the SB lead by Colonel Stanislaw Liskowski (Director of the Technical and Operational Department), Colonel Dionizzi Makzak (deputy director of the Operational Technique Department) and First Lieutenant Wlasislaw Novosad (translator) arrived in Romania for exchange of experience. The visit had the following objectives: 1) organizational structure and general problems on the technical - operative line; 2) visiting laboratories and production sectors within the Special Unit "P" and some exploit sectors within the "T" Special Unit; 3) presentation of OT (Operative Technique) carried out in the Special Unit "P" and discussions on them; 4) Visit of "T" compartments within county inspectorates; 5) exchange of equipment and documentation. DSS has sent free of charge a set of four elements comprising OT and the afferent documentation to the Polish delegation. In the relations plan of the Romanian Ministry of the Interior for 1977 were foreseen: the visit of a delegation of four specialists and a translator in the HPR at the beginning of 1977 and a visit by a Polish delegation to SRR In the same year[43].

In the 1980s there were also collaborations with the Hungarian security and intelligence services. Thus, on May 25, 1975 a delegation from the Special Unit "R" went for exchange of experience in the HPR. In January 1976, a meeting was held between representatives of DSS with Hungarian counterparts at CBCC (Common Border Crossing Point) Bors where the Romanian side handed OT equipment to the Hungarians. The Hungarian services asked the Romanian services for informative - operative information on two Hungarian citizens who met on Romania's territory with an American citizen[44].

---

41 BStU, MfS, ZAIG 7168, pp. 1-11, „KGB Report on New Elements in US Policy toward the European Socialist Countries", March 31, 1984, in *C.W.I.H.P.*
42 A.N.C.S.S.A., Documentary Fund, File Nº 10782, vol. 10, tabs 46-48, 52.
43 Ibidem, tabs 181-190.
44 A.N.C.S.S.A., Documentary Fund, File Nº 10782, vol. 11, tabs 61-64, 69, 83-89.

In 1976, OTTC (Operative Technique and Transmissions Commandment) visited SFRY, HPR and USSR[45].

Latest information exchanges of DSS with similar structures from WTO, recorded in official documents, refer to a visit to Sofia, on July 4, 1985, of a Romanian delegation composed of Iulian Vlad and Gheorghe Andreescu, where discussions took place on the exchange of information on the movement, on the territories of the two countries, of persons associated with Arab terrorist organizations. Vladimir Todorov and Martin Petkov, both from PGU, took part in the discussions[46]. In 1986, a collaboration protocol between DSS and KDS on the exchange of information and the taking of the necessary measures with regard to acts of terrorism was signed[47].

In the early 1980s, the position of KGB towards Romania has worsened, the Romanian state being characterized as an enemy state by both USSR as well as the other states in Soviet orbit. The "privileged" relationships between Bucharest and other capitals in the West and the Orient, especially Bonn, Washington and Beijing, worried the Kremlin leadership in an excessive manner. Moscow has sent clear directives to other fraternal states to retain maximum discretion in the execution of operations against Romania. Indeed, after the invasion of CSR, Moscow was careful to dissimulate misunderstandings with Bucharest. This is understandable since there is interest in the "Trojan Horse" thesis succeeding in the great Western chancelleries, while avoiding tactical countermeasures. Neither did Nicolae Ceausescu venture to upset USSR, as evidenced by the large number of double agents unmasked by Romanian counter-intelligence and sanctioned only by retirement or sending back "into production."

Through a document issued by the KGB in 1984 it was shown that Moscow initiated a series of bilateral and multilateral co-operation within the WTO informative community to which SRR was not invited because of Ceausescu's behaviour. The "quarantine" imposed on the Romanian state by USSR and its allies were part of the KGB-GRU plans of active measures as a counter-response to the dissidence displayed internationally by the authorities in Bucharest.

---

[45] Ibidem, vol. 11, tabs 289.

[46] The Committee for Disclosing the Documents and Announcing Affiliation of Bulgarian Citizens to the State Security and the Intelligence Services of the Bulgarian National Army (C.O.M.D.O.S.), Documentary Collections. *The Bulgarian State Security and the Intelligence Services of Eastern Bloc Countries (1944-1989)*. Bulagaria, Sofia, 2015, doc. nr. 271, pp. 1523-1529.

[47] Ibidem, doc. nr. 272, pp. 1530-1533.

Conclusions

The low level of collaboration between the Department of State Securitate and similar structures of the Warsaw Treaty Organization countries was not beneficial for the evolution of the Romanian institution after the change of the political regime in 1989. Documentary material available to research reveals a sinuous character with periods of bi- and multilateral co-operation coupled with inefficiency of the Department of State Securitate with homologous security and intelligence services. The inter-agency intelligence in Romania can be periodized as follows: an incipient phase (1945-1960) in which a "fraternal" cooperation was attempted, characterized by common operations and conscious exchanges of information; a period of tension (1960-1970) as a result of Romania's condemnation of the invasion of the troops of Warsaw Treaty member countries in Czechoslovakia, where information exchanges were more sporadic; a period of resuming collaborations at the level of the socialist block following the East-West (1970-1975) rebound when a closer approach to Romania was attempted; the last period that corresponds to the last communist decade finds the Department of State Securitate in an almost total isolation, which will be to the detriment of the Romanian intelligence services after 1989. I consider it plausible that the Department of State Securitate was unable to cooperate with the Soviet services around the events of December 1989 due to the fact that until then they were informative opponents.

Romania had a reaction to the Soviet-coordinated informational aggressions. I refer here to intelligence structures set up specifically for conducting actions to counteract informational aggression. Within the Romanian security and intelligence structures, an internal counter-intelligence service will be set up against the socialist countries, which will later become an independent military unit. In addition, in 1969, a Disinformation Service will be set up, 11 years after the establishment of a similar structure in the USSR. These two Romanian structures are real mechanisms for counteracting the informational war against Romania. I consider that through the scientific approach I have reduced the blurriness of this professional structure, whose activity has been for a while confined by people under its leadership. The decision to set up such an intelligence structure is the best example to characterize the degree of cooperation and friendship between the Securitate and similar services in the socialist countries.

References:

1. Andrew, Christopher, Mitrokhin, Vasili, (2005), *The World Was Going Our Way: The KGB and the Battle for the Third World*, New York, Basic Books.

2. Banu, Florian, (2015), „From collaboration to isolation. The relations between the Securitate with similar service of intelligence of the Warsaw Treaty Organization, 1955-1989, part I", in *Archives of Totalitarism*, Year XXIII, Nº 86-87, 1-2/2015.

3. Bittman, Ladislav, (1972), *The Deception Game: Czechoslovak Intelligence in Soviet Political Warfare*, Siracusa, Syracuse University Research Corporation, 1972.

4. Bulgarian Archive of the Ministry of the Interior, Sofia, Fond 2, Record 1, File N⁰ 1345, „Report from Gen. M. Spasov on Multilateral Security Meeting in Bucharest", March 12, 1958, in *C.W.I.H.P.* (Cold War International History Project); File N⁰ 1339, „Report on Visit to Romania on Counterintelligence Issues", March 23, 1959, in *C.W.I.H.P.*

5. Bulgarian Archive of the Ministry of the Interior, Sofia, Fond 1, Record 10, File N⁰ 338, „Correspondence between Gen. A. Solakov and Gen. K. Onescu on Acquired Intelligence Information", December 22, 1965, in *C.W.I.H.P.;* „Letter from Gen. A. Solakov to Gen. K. Onescu on Information on Italian Citizens", January 09, 1966, in *C.W.I.H.P.*

6. Mandrell, Paul, (2014), „Cooperation between HV A. and the KGB, 1951-1989", in *German Historical Institute Bulletin,* Richard F. Wetzell (ed.), Supplement 9 (2014).

7. National Central Historical Archives (N.C.H.A.), Central Committee of Romanian Comunist Party Fund (C.C. of R.C.P.), Administrative-Political Section, File Nº 13/1962, tabs 2-6; N.C.H.A., C.C. of R.C.P. – Writing Section Fund, File Nº 10/1963.

8. National Council for the Study of the Securitate Archives (N.C.S.S.A.), *The Party and the Securitate. The history of a failder idle (1948-1989)*, doc. Nº 91, Bucharest, Florian and Luminita Banu (eds.), Iasi, Editorial Demiurg House, 2013, pp. 351-355.

9. Olaru, Stejărel, Herbstritt, Georg, (2005), *Stasi and the Securitate*, Bucharest, Humanitas Publishing House.

10. Ritter, László, (2007), „The Soviet – Hungarian Intelligence Co-operation in the Early Cold War Period" in *NKVD/KGB Activities and its Cooperation with other Secret Services in Central and Eastern Europe 1945-1989*, Alexandra Grúňvá (ed.), Bratislava, 14-16th November 2007.

a. Romanian Intelligence Service, *The White Book of the Securitate*, vol. III, doc. Nº 13, 16, 18, Bucharest, 1995, pp. 154-156.

b. Troncotă, Cristian, (2014), *The Duplicitous: a history of security and intelligence services of the communist regime in Romania: 1965-1989*, second edition revised and added, Bucharest, Elion Publishing House.

11. The Archives of the National Council for the Study of the Securitate Archives (A.N.C.S.S.A.), Documentary Fund, File N° 88, vol. 4, tab 288; File N° 13134, vol. 28, tab 166, 201; File N° 10782, vol. 10, tabs 46-48, 52.

12. The Committee for Disclosing the Documents and Announcing Affiliation of Bulgarian Citizens to the State Security and the Intelligence Services of the Bulgarian National Army (C.O.M.D.O.S.), Documentary Collections. *The Bulgarian State Security and the Intelligence Services of Eastern Bloc Countries (1944-1989)*. Bulgaria, Sofia, 2015, doc. no. 271, pp. 1523-1529.

13. The Institute for the Study of Totalitarian Regimes of the Czech Republic, *Cooperation in the Eastern Bloc 1948-1989: documents on bilateral cooperation,* declassified 01.01.2008.

14. Watts, Larry L., (2011), *With Friends Like These...The Soviet Bloc's Clandestine War Against Romania*, english translation by Camelia Diaconescu, Bucharest, RAO Publishing House.

THE SPIES WHO DEFENDED US: SPY STORIES AND LEGITIMATING DISCOURSES IN CEAUŞESCU'S ROMANIA, 1965–77

Dragoş PETRESCU *

Abstract

The present paper analyses the intricate issue of legitimation of non-democratic regimes by focusing on the communist regime of Nicolae Ceauşescu during a particular time span, namely, 1965–77. This author contends that the issue of legitimation of communist rule in Romania should be addressed not only from the perspective of recent history and communist studies, but also from the perspective of history of intelligence. Thus, this paper demonstrates that in the particular context of August 1968, the Ceauşescu regime acquired "limited legitimacy through consent." Furthermore, from the perspective of history of intelligence, this paper argues that certain communist spy novels set forth fictional characters of Securitate officers as defenders of the Romanian "socialist nation" against the hostile actions of Western spies. Thus, for a limited period of time such spy novels contributed to persuading some segments of society to believe that the Securitate's mission was actually to protect the nation against foreign, that is, Western enemies.

Keywords*: 1968, legitimation, communism, Securitate, spy novels, role models*

Introduction

This paper addresses the intricate issue of legitimation of non-democratic regimes by focusing on the case of the communist regime of Nicolae Ceauşescu in Romania. The main argument set forth in my paper is that the Ceauşescu regime actually managed to achieve legitimacy, but a particular type of legitimacy, which can be termed following the British social theorist David Beetham as "limited legitimacy through consent." Ceauşescu lived his finest hour on Wednesday, 21 August 1968, when he publicly condemned the Soviet-led military invasion of Czechoslovakia. This gesture of defiance brought him and the Romanian Communist Party

* Prof. dr., University of Bucharest, dragos.petrescu@fspub.unibuc.ro

(RCP) a broad popular support and silenced the domestic critical voices towards the regime for many years.

Furthermore, the present paper argues that the immediate post-1968 context should be discussed from the perspective of the history of intelligence. This author contends that popular perceptions of the secret police apparatus deserve thorough investigation, all the more that in the post-1989 context research concentrated almost entirely on unmasking the wrongdoings of the Securitate. Thus, it is important to assess to what extent large strata of the population were persuaded to believe that the main purpose of the Securitate was to defend them from the hostile actions of Western spies. It may be argued that the communist spy novels featuring Securitate officers waging an „invisible war" against Western spies in order to defend the „achievements of socialism" supported the regime's efforts at legitimizing itself. To illustrate this argument, the present paper addresses the works and the main characters of the novels written by three generations of writers of spy novels in communist Romania (Theodor Constantin, Haralamb Zincă and Rodica Ojog-Braşoveanu).

On the Road to Absolute Power: Socialist Modernization, Nation-Building and Limited Legitimacy

After coming to power in March 1965, Ceauşescu basically followed the political strategy of his predecessor, Gheorghe Gheorghiu-Dej, based on cautious independence from Moscow and sustained industrialization. This was accompanied by a closely watched ideological relaxation combined with a modest improvement of the living standards of the population. As a consequence, popular perceptions of the regime improved gradually over the period March 1965–August 1968. The modest improvement of the standards of living of the population found an echo in the hearts and minds of a majority of Romania's population.[1] Thus, in August 1968 – ten years after the withdrawal of Soviet troops from Romania – when Ceauşescu gave his famous "balcony speech" in which he condemned the invasion of Czechoslovakia by the WTO troops, large segments of the population supported him without hesitation. The effect of Ceauşescu's discourse on Romania's population at large was enormous. Arguably, that speech represented for many Romanians the "proof" of Ceauşescu's charismatic

[1] For more on this, see Dragoş Petrescu, "Closely Watched Tourism: The Securitate as Warden of Transnational Encounters, 1967–69," *Journal of Contemporary History* (2015) Vol. 50, No. 2, pp. 341–345.

qualifications.[2] In fact, Ceauşescu's "charismatic leadership" – to use Reinhard Bendix's inspired term – emerged in the dramatic conditions of that August 1968.[3] At the same time, as David Beetham rightly argues, the use of the Weberian concept of "charismatic authority" is problematic in the sense that it "assigns far too exclusive an importance to the individual, and leads to fruitless, because unresolvable, disputes about whether particular leaders possess the indefinable quality of 'charisma' or not."[4] When analyzing the mechanism that provided the Ceauşescu regime with unprecedented mobilizing capacity one should concentrate on two major issues: (a) Ceauşescu's personality and leadership style; and (b) the particular circumstances in which popular mobilization occurred in 1968.

Ceauşescu was by far less flexible in adopting various policies than his predecessor, Gheorghiu-Dej. Nonetheless, he was only 47 when he became secretary general of the party and managed to build a positive image of himself as a "man of the people" by proceeding consistently to grassroots consultations. One can easily grasp the extent of the phenomenon from the large number of domestic mass rallies analysed above only for the period January-August 1968. During the period 1965–68, Ceauşescu's domestic visits were carefully staged and quite often he visited the most relevant historic monuments in the respective area, thus paying respect to the deeds of the ancestors with an emphasis on the medieval rulers of Romanian principalities. This was in sharp contrast with the leadership style of his predecessor, Gheorghiu-Dej, who did not champion such staged domestic visits. Furthermore, the launch of his belated and short lived de-Stalinization – which was intended primarily to unmask the wrongdoings of Gheorghiu-Dej and damage his legacy among the nomenklatura members – made of Ceauşescu the undisputed leader of the RCP.

Ceauşescu's policy of independence from Moscow and opening toward the West – which was initiated in fact by Gheorghiu-Dej – contributed decisively to the mass mobilization that followed his speech of 21 August 1968. In this respect, Ceauşescu benefited largely from the line inaugurated by Gheorghiu-Dej. Recollections by critical intellectuals, some of whom became after 1977

---

[2] According to Max Weber, charisma is: "A certain quality of an individual personality by virtue of which he is set apart from ordinary men and treated as endowed with supernatural, superhuman, or at least specifically exceptional powers or qualities." Quoted in Reinhard Bendix, "Reflections on Charismatic Leadership," in Reinhard Bendix et. al., eds., *State and Society: A Reader in Comparative Sociology* (Berkeley: University of California Press, 1973), p. 619.

[3] Bendix, "Reflections on Charismatic Leadership," pp. 616–629.

[4] David Beetham, *The Legitimation of Power* (London: Macmillan, 1991), p. 156.

fierce political opponents of the supreme leader of the RCP, support this argument. Writer Paul Goma, the initiator of the 1977 Goma movement for human rights and perhaps the most famous Romanian dissident, wrote about the atmosphere in Bucharest on 21 August 1968. According to Goma, Ceauşescu's appeal to the population to take arms and defend their country had a tremendous mobilizing force.[5] Writer Dumitru Ţepeneag remembers that Ceauşescu's discourse had an instantaneous effect on him: "For some days, I was a convinced Ceauşescuist."[6] A bitter confession by journalist Neculai Constantin Munteanu, who became one of the most acerbic critics of Ceauşescu's dictatorship as part of the Romanian desk of Radio Free Europe during the 1980s, deserves further examination. In 1977, Munteanu addressed a letter to Ceauşescu himself, in which he stated that he had decided to leave Romania forever and put forward his main reasons for making such a decision. In his letter, Munteanu also mentioned that on 21 August 1968, while he was in front of the CC building and listened to Ceauşescu's speech, he felt proud of being a Romanian: "The vehemence of your condemnation of the armed aggression of some member countries of the WTO against a friendly and allied country made me feel proud of being a Romanian."[7]

Simple themes, such as the struggle for independence and return to traditional values, found an echo in the minds and hearts of a majority of the Romanian population. At the same time, people could experience on an everyday basis a cautious ideological relaxation, a slight improvement of the living standards and an opening towards the West. In 1968, things seemed to move in the right direction, and many felt that the RCP leadership was truly concerned with improving the general situation of the population. Such a widespread positive perception of the regime permitted the RCP to achieve a "limited legitimation through consent."[8] Moreover, the "balcony speech" – which was generally perceived as a "proof" of Ceauşescu's charismatic qualifications – was given at the beginnings of his rule. At the same time, as Max Weber puts it, if a charismatic leader "is for long unsuccessful, above all if his leadership fails to benefit his followers, it is likely that his charismatic

---

[5] Paul Goma, *Amnezia la români* (Amnezia to Romanians) (Bucharest: Editura Litera, 1992), p. 54.
[6] Dumitru Ţepeneag, *Reîntoarcerea fiului la sînul mamei rătăcite* (The return of the son to prodigal mother's breast) (Iaşi: Institutul European, 1993), p. 95.
[7] Neculai Constantin Munteanu, *Ultimii şapte ani de-acasă: Un ziarist în dosarele Securităţii* (The last seven years at home: A journalist in the files of the Securitate) (Bucharest: Editura Curtea Veche, 2007), p. 120.
[8] Beetham, *The Legitimation of Power*, p. 117.

authority will disappear."[9] It took, however, more than ten years for Ceauşescu's charisma to erode.[10]

Spy Stories: Securitate Officers as Positive Role Models

From the history of intelligence perspective, it is relevant to assess popular perceptions of Securitate officers during the time interval 1968–77. As mentioned above, the concept of "limited legitimacy through consent" permits the study of legitimation processes under non-democratic regimes. In this respect, the case of Romania is relevant for the above-mentioned period because during that particular period a series of factors, such as economic improvement, ideological relaxation, cultural openness to the West or increased permeability of the borders for international tourism. Ceauşescu's nationalism also contributed in legitimizing the regime in the eyes of the population. Spy novels, though a minor literature genre, contributed significantly to this process of legitimation by setting forth role models which young audiences were eager to emulate. Fictional characters, communist spies on of the 007 kind thus emerged as daring defenders of the "achievements of socialism."

Given the technological backwardness of the Soviet bloc countries, one could ask nevertheless what were those "achievements of socialism" the Western spies were eager to steal and smuggle to the West. To this question, the authors of communist spy novels manage to find an answer, which at the time sounded convincing, including for this author. This answer reads as follows: in spite of the technological backwardness of communist Romania, under popular democracy the country has established a network of research institutes, which produce amazing research project with many practical applications. As a consequence, the plot of many spy novels published under communism revolves around the way the Securitate officers manage to hamper Western spies steal the results of cutting-edge research performed by research teams led by gifted Romanian scientists. This paper concentrates on the fictional characters developed by the most talented writers of spy novels in communist Romania, who at the same time represent three generations of writers: Theodor Constantin (1910–75); Haralamb Zincă (1923–2008); and Rodica Ojog-Braşoveanu (1939–2002).

Theodor Constantin published several spy and detective novels. One of the most successful spy novels is entitled *La miezul nopţii va cădea o stea* (A

[9] Quoted in Bendix, "Reflections on Charismatic Leadership," p. 620.
[10] For a detailed analysis of the meaning and consequences of Ceauşescu's gesture of defiance of August 1968, see Dragoş Petrescu, "Legitimacy, Nation-Building and Closure: Meanings and Consequences of the Romanian August of 1968," in M. Mark Stolarik, ed., *The Prague Spring and the Warsaw Pact Invasion of Czechoslovakia, 1968: Forty Years Later* (Mundelein, IL: Bolchazy-Carducci Publishers, 2010), pp. 237–259.

star will fall at midnight), whose plot is placed during WW II, in Transylvania, after the coup of 23 August 1944. Romania shifted sides and the Romanian army is engaged in war against Nazi Germany. In this context, the Romanian military intelligence eventually uncovers and annihilates an experienced Nazi spy infiltrated in the Romanian Cipher Section.[11] Subsequently, the novel was made into a movie, *Secretul cifrului* (The secret of the cipher), released in 1960, which was well received by the public considering the limited offer of action movies in Romania at the time.[12] Theodor Constantin wrote both spy and detective novels, and some of the main characters of his novels, Securitate and Militia officers, sometimes collaborate in solving difficult cases. In terms of propaganda and ideology, the author uses arguments related to class struggle and antifascism (*La miezul nopţii va cădea o stea*, *Fiul lui Monte Cristo*) or to the critique of the interwar "bourgeois" political system and the institution of monarchy (*Urmărirea abia începe*).[13] The main character of his most successful spy novels, which are those featuring an international spy agency called the Nebel Trust, is the Securitate Major Radu "Ducu" Mănăilă.

"Ducu" Mănăilă featured first in the novel *Fiul lui Monte Cristo* (Son of Monte Cristo) published in 1958.[14] The novel covers the period 1937–50 and takes place in Brăila, the author's native town. Ducu, who comes from a modest, working-class family is seventeen and falls in love with Ingrid Richter, the daughter of a wealthy Swiss businessman. Ducu's father – nicknamed Monte Cristo – is assassinated. After a while, Ducu finds out that Ingrid's father, whose real name is Walther, is a Nazi spy and the assassin of Monte Cristo. Walter puts an end to the love story between his daughter and Ducu by sending Ingrid abroad to continue her studies. Eventually, Ducu prompts Walter to commit suicide by threatening to unmask him as a Nazi spy. After the coup of 23 August 1944, Ducu joins the army and fights against the Nazis and, after the communist takeover and the establishment of the Securitate, he enters the secret police apparatus. While on secret mission in Switzerland, Ducu meets Ingrid, now married and mother of a boy, and realizes that their love story ended for good.

The novel *Doamna în mov* (Lady in purple), was published in 1966, during the Ceauşescu period. The Securitate Major Radu "Ducu" Mănăilă is

---

[11] Theodor Constantin, *La miezul nopţii va cădea o stea* (A star will fall at midnight) 3rd revised ed. (Bucharest: Editura Tineretului, 1962).
[12] Lucian Bratu, *Secretul cifrului* (The secret of the cipher), Romania, 79 min., 1960.
[13] Theodor Constantin, *Urmărirea abia începe* (The chase has only started) 2nd ed. (Bucharest: Editura Militară, 1963).
[14] Theodor Constantin, *Fiul lui Monte Cristo* (Son of Monte Cristo) (Bucharest: Editura Tineretului, 1958).

briefed by his superiors that the Nebel Trust intends to steal the results of the "secret research" performed by a team headed by Alcibiade Robescu, from the Romanian Academy, regarding the military uses of a laser device.[15] While Major Mănăilă works on the case, he finds out that the Nebel Trust sent to Romania one its most experienced spies. Eventually, Mănăilă finds out that the agent is a woman, actually Ingrid, his only true love, but does not hesitate to arrest her. Once unmasked, Ingrid commits suicide.

Haralamb Zincă is the pen name of Hary Isac Zilberman (1923–2008), an author who also wrote spy and detective novels. His most successful spy novel is *Moartea vine pe bandă de magnetofon* (Death comes on magnetic reel-to-reel tape),[16] which was made into a movie released under the title *Un om în loden* (A man in loden overcoat).[17] The main characters are two Securitate officers, Captain Lucian and Lieutenant Frunză, who have to solve the case of engineer Dan Stamatiad, who had received several death threats. Stamatiad, a gifted geologist, was involved in a major geological survey codenamed "U-74" aiming at mapping the uranium ore deposits in Romania. Zincă draws a bright portrait of a Securitate officer in the early Ceaușescu epoch. For instance, Captain Lucian calms down Stamatiad, who was deeply disturbed by the death threats received, with the following words: "Please be assured that, from this moment on, *you are not alone anymore*… Please do understand, no matter if this is a joke or not, *you are not alone anymore.* This case will be given our outmost care [original emphasis]."[18] In ideological terms, Zincă depicts the "new" Securitate, close to the people and "defender of socialism," in line with the tenets of Ceaușescu's national-communism and in contradistinction with the "old" Securitate from the time of Gheorghe-Gheorghiu-Dej, which was allegedly under Moscow's control. Turning back to the above-mentioned novel, the two Securitate officers manage, quite obviously to solve the thorny case of industrial espionage. The spies are unmasked and caught, and it turns out that it was about an organization specialized in industrial espionage founded in the West by a former Iron Guard member under the cover of an antique business company named Venus of Milo.[19]

Rodica Ojog-Brașoveanu (1939–2002) is perhaps the author who proposed to her readers the most interesting fictional characters of spy and

---

[15] Theodor Constantin, *Doamna în mov* (Lady in purple) (Bucharest: Editura Tineretului, 1966), pp. 33–34.
[16] Haralamb Zincă, *Moartea vine pe bandă de magnetofon*, (Death comes on magnetic reel-to-reel tape) (Bucharest: Editura Militară, 1967). As for Zincă's detective novels, see, for instance, *Ochii doctorului King*, (Doctor King's eyes) 2nd ed. (Bucharest: Editura Militară, 1972).
[17] Nicolae Mărgineanu, *Un om în loden* (A man in loden overcoat), Romania, 78 min., 1979.
[18] Haralamb Zincă, *Moartea vine pe bandă de magnetofon*, pp. 25–26.
[19] Ibid., p. 266.

detective novels in communist Romania. Ojog-Braşoveanu differs fundamentally from other authors in the field due to the narrative keys she uses, that is, comedy and irony. Although her novels feature Securitate and Militia officers and are set in the particular context of Ceauşescu's Romania, her spy and detective novels proved to be successful with the generations born after the fall of communism and who learned in school about the systematic violation of fundamental human rights under the communist dictatorship.[20]

The most interesting character of Ojog-Braşoveanu's spy novels is the Securitate Major Minerva Tutovan, who teams up with Lieutenant Vasile Dobrescu to counteract Western spies. It may be argued that Major Tutovan epitomizes the "new" and national Securitate established after Ceauşescu's coming to power, but in a more imaginative and less ideological way as compared to the fictional characters in Zincă's novels. Major Tutovan is a woman and, even more importantly, is someone from among "us" who decided to work for "them" in order to defend her country and ours. This is how the argument between the lines reads.[21]

It is worth mentioning the dedication to one of her early works, *Omul de la capătul firului* (The man at the other end of the line), in which the author states that the book is dedicated to the "anonymous heroes fighting on the invisible front of counter-intelligence" on the occasion of celebrating 25 years from the establishment of the Securitate on 30 August 1973.[22] Major Tutovan used to teach Mathematics in a Bucharest high school and was feared for her severity. She was recruited after solving a murder case while on thematic trip nearby Bucharest with her pupils.[23] The success of Ojog-Braşoveanu's novels is also due to the unusual team Tutovan-Dobrescu, given the fact that Tutovan was Dobrescu's teacher in high school and he had great difficulty in taking a passing grade since he was not exactly gifted for Mathematics.[24]

At the same time, the spy novels by Ojog-Braşoveanu does not depart from the recipe used by most writers of the genre in communist Romania. Thus, the results of fundamental research performed by state institutes

---

[20] See in particular the collection Rodica Ojog-Braşoveanu (on paper an in E-book format) established by Editura Nemira; accessed 4 September 2017 at https://nemira.ro/catalogsearch/result/?q=ojog+brasoveanu&cat=; accessed on 4 September 2017.

[21] One should also mention Ojog-Braşoveanu's detective novels whose main character is Melania Lupu, an old lady whose way of lessening boredom is to involve herself in economic crimes.

[22] Ojog-Braşoveanu, *Omul de la capătul firului* (The man at the other end of the line) (Bucharest: Editura Albatros, 1973). The novel was made into a movie. See Geo Saizescu, *Şantaj* (Blackmail), Romania, 95 min., 1982.

[23] Ojog-Braşoveanu, *Omul de la capătul firului*, pp. 17–18.

[24] Ojog-Braşoveanu, *Spionaj la mănăstire* (Espionage at the monastery) (Bucharest: Editura Militară, 1972), p. 10.

remains the main objective of Western espionage. For instance, in the spy novel *Spionaj la mănăstire* (Espionage at the monastery), Major Tutovan and Lieutenant Dobrescu mange to hamper the stealing and smuggling across the border of a revolutionary anesthetic developed by a Romanian team headed by professor Lucaci. An international organization specialized in industrial espionage, the TEX Trust, sends an agent to Romania. The agent is a gorgeous but also extremely clever young woman, Nora Roman.[25] Major Tutovan is not able to hamper the assassination of professor Lucaci, but succeeds in unmasking the Western spy and hampering the smuggling of the precious formula across the border.

Concluding remarks

This paper has focused on the period 1965–77, a period in which the communist regime in Romanian displayed a less ferocious face and which is associated in the folk memory with economic improvement and ideological relaxation. The main argument set forth by this paper is that the Ceauşescu regime actually managed to achieve legitimacy, but a particular type of legitimacy, which can be termed following the British social theorist David Beetham as „limited legitimacy through consent." Ceauşescu lived his finest hour on Wednesday, 21 August 1968, when he publicly condemned the Soviet-led military invasion of Czechoslovakia. This gesture of defiance brought him and the Romanian Communist Party a broad popular support and silenced the domestic critical voices towards the regime for many years.

At the same time, this author has demonstrated that the immediate post-1968 context deserves to be analysed from the perspective of the history of intelligence, more precisely, by examining popular perceptions of the secret police apparatus and thus shed more light on the legitimizing process mentioned above. In this respect, the present paper has shown that communist spy novels featuring Securitate officers waging an „invisible war" against Western spies to defend the „achievements of socialism" supported the regime's efforts at legitimizing itself. This paper has discussed the works and the main characters of the novels written by three generations of writers of spy novels in communist Romania (Theodor Constantin, Haralamb Zincă and Rodica Ojog-Braşoveanu). The analysis has also revealed that a process of memory borrowing emerged after 1989, which deserves to be further investigated by corroborating recollections posted on the Internet and reception of certain communist spy novels after 1989 by generations born after the fall of the communist regime.

[25] Ibid., p. 187 and pp. 194–202.

References:

1. Beetham, David, *The Legitimation of Power* (London: Macmillan, 1991).
2. Bendix, Reinhard, "Reflections on Charismatic Leadership," in Reinhard Bendix et. al., eds., *State and Society: A Reader in Comparative Sociology* (Berkeley: University of California Press, 1973).
3. Bratu, Lucian, *Secretul cifrului* (The secret of the cipher), Romania, 79 min., 1960.
4. Constantin, Theodor, *La miezul nopţii va cădea o stea* (A star will fall at midnight) 3rd revised ed. (Bucharest: Editura Tineretului, 1962).
5. Constantin, Theodor, *Urmărirea abia începe* (The chase has only started) 2nd ed. (Bucharest: Editura Militară, 1963).
6. Constantin, Theodor, *Fiul lui Monte Cristo* (Son of Monte Cristo) (Bucharest: Editura Tineretului, 1958).
7. Constantin, Theodor, *Doamna în mov* (Lady in purple) (Bucharest: Editura Tineretului, 1966).
8. Goma, Paul, *Amnezia la români* (Amnezia to Romanians) (Bucharest: Editura Litera, 1992).
9. Mărgineanu, Nicolae, *Un om în loden* (A man in loden overcoat), Romania, 78 min., 1979.
10. Munteanu, Neculai Constantin, *Ultimii şapte ani de-acasă: Un ziarist în dosarele Securităţii* (The last seven years at home: A journalist in the files of the Securitate) (Bucharest: Editura Curtea Veche, 2007).
11. *Ochii doctorului King*, (Doctor King's eyes) 2nd ed. (Bucharest: Editura Militară, 1972).
12. Ojog-Braşoveanu, Rodica, *Omul de la capătul firului* (The man at the other end of the line) (Bucharest: Editura Albatros, 1973).
13. Ojog-Braşoveanu, Rodica, *Spionaj la mănăstire* (Espionage at the monastery) (Bucharest: Editura Militară, 1972).
14. Petrescu, Dragoş, "Closely Watched Tourism: The Securitate as Warden of Transnational Encounters, 1967–69," *Journal of Contemporary History* (2015) Vol. 50, No. 2, pp. 341–345.
15. Petrescu, Dragoş,"Legitimacy, Nation-Building and Closure: Meanings and Consequences of the Romanian August of 1968," in M. Mark Stolarik, ed., *The Prague Spring and the Warsaw Pact Invasion of Czechoslovakia, 1968: Forty Years Later* (Mundelein, IL: Bolchazy-Carducci Publishers, 2010), pp. 237–259.
16. Saizescu, Geo, *Şantaj* (Blackmail), Romania, 95 min., 1982.
17. Ţepeneag, Dumitru, *Reîntoarcerea fiului la sînul mamei rătăcite* (The return of the son to prodigal mother's breast) (Iaşi: Institutul European, 1993).
18. Zincă, Haralamb, *Moartea vine pe bandă de magnetofon*, (Death comes on magnetic reel-to-reel tape) (Bucharest: Editura Militară, 1967).

PORTRAITS, ESSAYS AND INTERVIEWS

TRUMP, NIXON, AND THE CIA[1]

Christopher MORAN*

Richard J. ALDRICH**

Introduction

"Unproductive", "disloyal", "what the hell do those clowns do out there in Langley". Richard Nixon, the 37th President of the United States, had some fairly waspish things to say about the Central Intelligence Agency (CIA). Nearly 50 years later, so too does the latest resident of 1600 Pennsylvania Avenue, Donald J. Trump. In the 10 months or so since winning the 2016 presidential election against his Democratic opponent Hillary Clinton, the bombastic New York businessman has called CIA officers "politically motivated" and "sick people" who peddle "fake news", and even equated the Agency with Nazi Germany. In his attitude towards the Agency, Trump is compelling reminiscent of Nixon, albeit with one big difference: while the latter expressed his feelings privately in the Oval Office, to be combed over by historians decades later, Trump – the self-appointed "Ernest Hemingway of a hundred and forty characters" – has made his animus towards the CIA public knowledge in real time, thanks largely to a series of early-morning social media tirades.

Many writers have acknowledged the similarities between Trump and Nixon: indeed, a cover of *New York* magazine featured a suited and red-tied Trump photo shopped as a latter-day "Tricky Dicky", throwing his arms open in his trademark "V" for victory salute. Google "Nixon and Trump" and nearly 16 million websites come up, pointing out the myriad of parallels: their appeal to the blue-collar forgotten man – the silent majority; their uneasy relationship with the press; their love of rough and tumble verbal sparring; their belief that foreign policy negotiating leverage is increased if your opponent thinks you are a "mad man" who might go nuclear; and their paranoid view that everyone who isn't with them is against them. What is striking, however, is that scant attention has been given to the striking similarities in their feelings towards, and dealings with, the CIA. It is argued

[1] A version of this article has already been published: see Christopher Moran & Richard J. Aldrich, 'Borrowing from Nixon's Playbook: Trump and the CIA', *Foreign Affairs*, Online 24 April 2017.

* Christopher R. Moran, is a Reader in US National Security at the Warwick University

** Richard J. Aldrich is a Professor of International Security at the University of Warwick

here that by understanding the dynamics that existed during the Nixon administration, we have a useful frame of reference for what might develop over the next few years.

***

Underpinning Trump's hostility is a seemingly unshakeable belief that the Agency is against him politically. Arguably, it is not hard to see why he might feel this way. Before the election, many senior intelligence officers like John Brennan, Jim Clapper, and Michael Hayden openly came out in favour of his rival Hillary Clinton, in doing so turning their back on the tradition that spies should remain neutral on political matters. Since then, the CIA has spearheaded investigations into possible links between Trump, his advisers, and Russian premier Vladimir Putin. Former acting CIA Director Michael Morell even accused Trump of being an "unwitting agent of the Russian Federation", an accusation, interestingly he has subsequently walked back on. Previously a fringe subculture, an amorphous movement known as the "Alt-Right" has burst onto the national stage, to some extent keeping the "CIA bogey" alive, penning story after story, tweet after tweet, about embittered Obama holdovers at Langley waging guerrilla warfare against the new president.

Trump's view that CIA is a political enemy has strong echoes of Richard Nixon. In 1950s, as Eisenhower's Vice-President, the hawkish Cold Warrior Nixon had enjoyed amicable relations with the CIA and its virulently anti-communist Director Allen Dulles, but the relationship soured with John F. Kennedy's narrow election victory in 1960. To his dying day, Nixon believed that Dulles, when briefing Kennedy, deliberately failed to refute the young senator's public statements and taunts about America slipping behind in the arms race, the so-called "Missile Gap". For Nixon, the belief that the CIA had some sort of political vendetta against him had a significant social dimension, stemming from a chip on his shoulder about the class of people who dominated the Cold War national security state, especially the CIA. As the son of poor small town grocer from Yorba Linda, California, he looked at the CIA with a fair degree of contempt, populated as it was then by veterans of the "Oh So Social" wartime Office of Strategic Services (OSS) – fashionable and silver-spooned Ivy Leaguers who, at their Georgetown cocktail parties, he imagined eulogising about Kennedy and snobbishly poking fun at social climbers like himself.

Trump has been notably critical of the CIA's performance. At campaign events, he regularly attacked the CIA for its faulty intelligence on Iraqi Weapons of Mass Destruction (WMD), which paved the way for the invasion of the country in 2003. Elsewhere, controversially, he suggested that WikiLeaks has better intelligence than the Agency. To the horror of many CIA

professionals, he said on television that he may or may not read the Presidential Daily Brief (PDB), stating that once or twice a week was enough for a "smart guy" like himself. Given the dangers faced by some CIA officers to acquire this information, Trump's remarks were insensitive at best.

Here, again, there are similarities with Nixon. Nixon regularly complained about CIA assessments of world affairs, lamenting that Agency estimators sat on the fence to avoid being blamed if they were wrong. On one occasion, after the CIA had failed to inform him that there had been a coup in Cambodia, he let rip at White House Chief of Staff Bob Haldeman: "Get rid of the clowns. What use are they? They've got 40,000 people over there reading newspapers." Like Trump, there is evidence that Nixon did not read the Daily Brief, at least not religiously. When, in 1970, an NSC staffer examined the briefs sent to Nixon during the previous year, he observed that the president's comments in the margins dwindled with every passing week, before vanishing completely.

***

Recognizing, then, that there are parallels between Trumps' view of the CIA and Nixon's, we would like to make some predictions about how CIA-White House relations might develop during the Trump administration.

It is likely, we would argue, that Trump will imitate Nixon by relying less on intelligence from the CIA and more on information from trusted White House advisers and ideologically-aligned external think tanks. Nixon's preference was to be briefed by his National Security Adviser, Henry Kissinger, rather than the Director of the CIA. Indeed, Kissinger recruited and employed his own group of analysts who produced their own version of the PDB. Amazingly, Nixon tried to exclude CIA Director Richard Helms from attending meetings of the National Security Council (NSC). On many major foreign policy issues, from rapprochement with China to the secret bombing of Cambodia, Nixon kept the CIA in the dark. Kissinger later admitted that this was "demoralizing" for the Agency and unlikely to be taught in manuals on best practice in public administration.

Nearly a year into his presidency, Trump has followed a similar path to Nixon, keeping foreign policy decision-making within an inner sanctum of largely political advisers with no intelligence background. One example of this was the (albeit brief) elevation of then presidential strategist Steve Bannon onto the influential "principals committee" of the NSC, while demoting the committee status of both the Director of National Intelligence (DNI) and the Chairman of the Joint Chiefs of Staff. The promotion of Bannon, a former investment banker and the driving force behind the ultra-conservative Brietbart News website, to a rank on the NSC equivalent to the Secretary of

State and above the country's top intelligence advisers sent shockwaves through political Washington. Although Bannon was later removed from the Committee and indeed later removed from the White House altogether, the episode provided a fascinating insight into Trump's thinking, specifically his desire to circumvent the CIA on national security decision-making.

***

Evidence suggests that Trump will at some stage look to reform the CIA, with the objective of turning it into a more obedient presidential tool. Such a move would be straight out of the Nixon playbook. In late 1970, fuelled by suspicions about the Agency's loyalty and efficiency, Nixon tasked James Schlesinger, then a renowned budget-cutter at the Office of Management and Budget, with carrying out a review of the CIA. Six months later, Schlesinger reported that the CIA had failed to adapt to the times, partly because it still recruited from a narrow Ivy League social base, and partly because it had been slow to grasp the potential of new technologies. To modernize the CIA and render it more attune to his worldview, Nixon eventually installed Schlesinger as CIA Director, in the process firing respected career intelligence professional Richard Helms. At Langley, Schlesinger's first words were "I'm here to make sure you don't screw Richard Nixon." In six short and stormy months at CIA, he sacked nearly 7% of the CIA's workforce, with the disproportionate share of the cuts being made in the Clandestine Division, the CIA's beating heart. Unsurprisingly, Schlesinger ranks as the least popular director in CIA history, with Porter Goss (2004-06), another interloper and perceived political hatchet man, in second place.

Annoyed and frustrated by intelligence assessments that contradict his policy preferences, especially in relation to Russia and his "America First" agenda, Trump has made no secret of his desire to reform and streamline the intelligence community. Before the inauguration, a source close to Trump told the *Wall Street Journal* that the CIA would be "slimmed down", with personnel levels cut and more staff uprooted from Agency headquarters in leafy suburbia to field postings around the world. Like Nixon with Schlesinger, we should expect Trump to appoint an intelligence outsider to lead such an effort. Indeed, Stephen Feinberg, a New York-based private equity executive, has been mentioned as a possible chairman, at least if Beltway backchat is to be believed.

Rather like Nixon before him, the worry among intelligence professionals who hold that the CIA should avoid a direct role in policy is that Trump is keen to create the conditions that will allow for CIA analysis to be moulded to support his world view. Despite being a critic of what he perceived as a liberal bias at CIA during the Obama years – evidenced by Director Brennan's public

support for the Iran Deal – Trump has laid the ground for politicized intelligence reporting of his own. His first visit to Langley was a gross display of politicization. Positioned in front of the Memorial Wall, a shrine to a hundred-plus of the Agency's lost heroes, he engaged in political grandstanding, boasting that his inauguration crowd had been more than Obama's in 2008 (incorrect), and stating (also incorrectly) that "almost everybody" in the room had voted for him. The message was one of, "get behind me, or get out"; Brennan called it a "despicable display of self-aggrandizement". Meanwhile, hawkish Kansas congressmen and Tea Party follower Mike Pompeo is perhaps the most openly partisan spy chief to ever lead the Agency. As a vocal member of the Republican-led House Select Committee inquiry into the deadly attack on the US consulate in Benghazi, Libya, in 2012, he was accused of politicizing the tragedy and turning it into a political hit job to bring down Hillary Clinton. Publicly, he has snapped with reporters who ask questions about Russian interference in the presidential election. Privately, in Cabinet meetings, he lends his opinion to matters far removed from national security, like health care. He also appears to have swallowed the staples of Trump's vocabulary, using words like "action" and "winning".

Anecdotally, there are suggestions that politicization of intelligence has already commenced. In spring 2016 – in an illustration of what Mark Lowenthal describes as "downward flowing politicization" (i.e., the policymaker telling the agency the analytical outcome they desire) – the media reported that the administration had sought to enlist the CIA and the Department of Homeland Security to build a case retrospectively for its controversial travel ban targeting citizens from seven majority-Muslim countries. Neither were said to be consulted before the immigration order was pushed out of the door; but, seemingly, both were expected to help Trump fulfill one his main and most ideological campaign promises. The dangers of a president strong-arming intelligence professionals to adopt certain predetermined policy positions need not be elaborated here: suffice is to say that with so many delicate security challenges facing the US – from an emboldened Russia threatening NATO allies in the Baltic and allying itself with Bashar al-Assad's brutal regime in Syria, to Iran being on a slow but certain cadence to obtaining nuclear weapons – it is essential that the intelligence community is not a policy echo chamber and is allowed to deliver hard truths and alternative models unvarnished by political persuasion.

Most worrying is the prospect of politicized covert action. Nixon overturned the government in Bolivia in 1971 partly because he had memories of visiting the country as Eisenhower's Vice President and being pelted with rocks by an angry leftist mob. Thin-skinned to the extent that is a major psychological weak spot, one worries that Trump could use the CIA for similar score-settling abroad. This is a scary thought given that since 9/11, the

CIA has become much more "weaponized", with drones, elite special forces, and powerful cyber-warfare weaponry.

***

Belittled with innuendo and ad hominems; marginalized from the centre of power; pressurized to toe the political line: it is interesting to speculate how the Agency will respond to an undoubted low ebb in CIA-White House relations. Michael Morell has forecast a "wave of resignations". History, however, tells us that this will not be the case. Up against a similarly antagonistic figure in Nixon, CIA officers refused to lay down, choosing instead to be resilient and fight back. Rather than pursuing direct confrontation, their approach was more subtle, covert and disguised, comparable to what anthropologist James C. Scott has called "everyday resistance" or "infrapolitics".

Down among the lower orders, infrapolitical activism involved leaving malicious comments about the president on noticeboards, as well as vandalizing Schlesinger's official portrait. Indeed, to stop the vandals, Schlesinger had to install a CCTV camera on the wall next to the picture. Among the CIA's senior managers, who resided in the seventh-floor executive offices, activism took the form of withholding information from the president. In 1971, for example, Britain's Security Service (MI5) "turned" KGB officer Oleg Lyalin and sent intelligence digests of his material to the FBI for onward circulation to the CIA and then the president. When FBI Director J. Edgar Hoover asked Nixon if he liked the reports, the latter replied, "What reports?" For a long time, despite repeated requests from the White House, the CIA's top brass refused to hand over any files detailing efforts to remove Cuban revolutionary Fidel Castro, perhaps fearing that Nixon would use them for blackmail purposes. "Those bastards in Langley are holding back something", fumed Nixon aide John Ehrlichman, "They just dig their heels in and say the President can't have it. Imagine that! The Commander-in-Chief wants to see a document, and the spooks say he can't have it".

Other forms of resistance took on a darker edge. Famously, elements within the intelligence community bedevilled Nixon's administration with leaks, the most significant coming from Deputy Ditector of the FBI Mark Felt, who, until he reached his nineties and revealed himself as Bob Woodward's golden source behind some of the early Watergate revelations, was known to the public only as "Deep Throat". Less famously, Admiral Thomas Moorer, the Chairman of the Joint Chiefs of Staff, planted a spy in Nixon's NSC. By his own admission, that spy (Yeoman Charles Edward Radford) photocopied "thousands, just thousands" of documents for Moorer.

It appears that Trump has awakened similar forces of resistance. To quote Senate Minority leader Chuck Schumer, "You take on the intelligence

community and they have six ways from Sunday of getting back at you". There have been numerous stories in the media of intelligence agencies hiding information from the president; in addition, we know that the CIA has denied security clearances to some of Trump's staff.

Analogous to the Nixon era, it appears that a key weapon in the secret state's arsenal of resistance will be leaks. From the moment he entered the White House, Trump has been besieged by illicit disclosures of sensitive information, from details of his telephone calls with foreign statesmen, to drafts of his executive orders on immigration and the possible revival of enhanced interrogation techniques against enemy combatants. Leaks have already claimed a high-profile victim in former National Security Adviser Mike Flynn, who was compelled to resign when details were leaked about a telephone conversation he had with a Russian diplomat prior to Trump's inauguration. Tellingly, perhaps, the story originated in the *Washington Post* with a piece by David Ignatius, who is well-known for his CIA sources. For angry intelligence officers, there is no doubting that Flynn's resignation was a significant coup. Since retiring from the military, Flynn has been a fierce critic of the CIA, accusing it of being a political tool of the Obama administration, and suggesting that in playing down warnings about terrorism from when he was Director of the Defense Intelligence Agency (DIA), it enabled the rise of the Islamic State in the Middle East. A long time Trump ally, he also led chants of "lock her up", directed at Hillary Clinton, at the summer 2016 Republication National Convention. In short, he was an attractive target.

The leaks that have plagued Trump's presidency, plus their early success in removing Flynn, have generated a vogue for the theory of the "Deep State": an evil nexus of institutions – corporate media, Wall Street, Silicon Valley, the intelligence community, the federal bureaucracy – that operate outside the democratic system conspiring to destabilize, smear, and coerce the president. The latest fillip to this belief is the President's extraordinary claim that his predecessor had bugged his Manhattan HQ, Trump Tower, in the weeks leading up to the election. Trump himself has thus far refrained from using the term, at least in public, leaving the brush fire building about Deep State infestation to proxies that include the right-wing media; trusted aides like Newt Gingrich ("Of course the Deep State exists"); and, for different ideological reasons, leftist critics such as Glenn Greenwald fearful of runaway intelligence agencies. So far, the main target of Trump's public complaints about leaks has been the CIA, especially outgoing Director John Brennan. "Was this the leaker of Fake News?", he tweeted, in reference to Brennan, after the release of a salacious dossier by an ex-MI6 officer detailing his trips to Moscow and hotel room peccadilloes.

How Trump manages leaks is likely to be one of the most important challenges he faces as president. Right now, in America, some 5.1 million

people have security clearances, a consequence of the "Need to Share" culture that has swept across the national security realm since 9/11. Chances are, therefore, that further unauthorized disclosures will occur. Nixon was destroyed by leaks: they consumed him. While he didn't rage about them 140 characters at a time, he did try to stop them, with disastrous consequences. Under Nixon, the war on leakers went to absurd lengths, allegedly prompting him even to discuss the possible poisoning of Jack Anderson, one of Washington's more flamboyant investigative reporters. Kissinger was, if anything, even more paranoid than Nixon, gradually telling the CIA less and less in the hope of starving journalists like Seymour Hersh; then, as now, the tactic did not work. Famously, of course, in a bid to stop the leaks, Nixon ordered wiretaps, black-bag jobs, burglaries, surveillance, and mail opening against perceived enemies. He also authorised the creation of a "special investigations unit", later nicknamed the "Plumbers", to root out leakers and find incriminating information on political opponents. Together, these illegal efforts would ultimately lead to his resignation in disgrace.

As Trump grapples with the problem of leaks, perhaps he should reflect on Nixon's experience. Clearly, he would be wise not to employ measures that cross the line, as Nixon's did, into illegality. To date, and true to form, he has come out swinging, like a bareknuckle brawler, calling on the Justice Department and FBI to investigate "low-life leakers" in the government. Meanwhile, in what appears like a two-pronged strategy, his surrogates double down on the idea of the Deep State, dragging the concept from conspiracy-laden websites like Infowars into broader public discourse. By mainstreaming and normalizing fears about a shadow network of spies and bureaucrats, the administration presumably hopes to win public acquiescence for its domestic program, which includes radical restructuring of the federal bureaucracy. Nixon's saving grace was a highly intelligent, if eccentric, National Security Advisor. Recently, Trump has also been forced to professionalise his senior appointments around the National Security Council, notably with the appointment of General H.R. McMaster. Even Senator John McCain, the Republican chairman of the Armed Services Committee and frequent Trump critic, called McMaster an "outstanding choice" adding that "he is a man of genuine intellect, character and ability". However, to properly stem the tide of leaks, the main lesson of the Nixon era is that Trump must repair his relationship with the intelligence community, especially the CIA, which is currently broken. If he continues to bully, disparage and outflank them like he would contestants on a reality TV show, the rift will widen and infrapolitical resistance will continue. He cannot say he hasn't been warned.

The „Journal of Intelligence History": reading recommendations

(by **Sorin APARASCHIVEI**)

The latest issue of the well-known *Journal of Intelligence History,* the official publication of the International Intelligence History Association (IIHA) contains the following articles: John Moran's *British military intelligence in aid of the civil power in England and Wales*; Rhodri Jeffrey-Jones' *The sensitivity of SIGINT: Sir Alfred Ewing's lecture on room 40 in 1927*, John Matz' *The Konnov/Mikhailov/Bakourskii espionage crises of July-August 1947 and Vyshinskii note on Raoul Wallenberg*, Adam Leong Kok Wey's *Japanese intelligence and covert operations: a strategic evaluation of Fujiwara Kikan in the invasion of Malaya and Singapore*, 1941-1942; Giovanni Coletta's *Politicising intelligence: what went wrong with the UK and US assessments on Iraqi WMD in 2002*, and a review article entitled *The Gatekeepers: film, television series, and book review*, signed by Eyal Paskovich. Inciting titles and well-known authors entice the reader to deepen his knowledge of historical events involving intelligence services.

Without reducing the importance of one or another articles mentioned we would like to emphasize that signed by Jon Moran, entitled *British military intelligence in aid of the civil power in England and Wales.* In this article, the author attempts to uncover the beginning of the intelligence cooperation between the British Army and the state's civilian and administrative institutions at the end of the XIX century and the beginning of the XX. This aspect is remarkably lacking in Romanian intelligence historiography.

According to Jon Moran, to deeply understand the creation of the modern intelligence structures, one needs to emphasize the role played by the representatives of civil authorities, that is mayors, prefects, junior prefects and local police chiefs, given that these local magistrates are the main guarantors of public order and the primary holders of information on state security.

In order to reconstruct the mechanism of intelligence collection, Jon Moran advises one to look at the legal framework on public gatherings valid during that period and at the way that state structures were mandated to intervene in cases of social disorder, rebellion, anarchist movements, attacks and strikes. The author notices the British did not have a military organization to permanently and systematically collect intelligence, which was initially done by local organs of civil intelligence. Hoping that we have sparked your interest for this issue of the *Journal of Intelligence History,* we wish you a pleasant reading.

Sorin APARASCHIVEI şi Florin-Badea PINTILIE,
Din istoria oficială a contraspionajului românesc,
Editura ANIMV, Bucureşti, 2018

(prezentare de **Codruţ LUCINESCU**)

O apariţie editorială de interes major atât pentru cercetătorii domeniului serviciilor secrete cât şi pentru publicul larg o constituie volumul *Din istoria oficială a contraspionajului românesc, perioada 1918 – 1945*.

Lucrarea, rodul a ani de cercetare sistematică în Arhiva Serviciului Român de Informaţii şi Arhivele Naţionale ale României urmăreşte să recreeze o imagine cât mai apropiată de realitatea epocii şi să reliefeze importanţa activităţii de contraspionaj în activitatea generală a structurilor informative româneşti, în deceniile analizate.

Autorii aduc în circuitul ştiinţific, pentru prima oară numeroase documente originale, ceea ce constituie un evident salt calitativ în laboriosul proces de reconstituire a adevărului istoric într-o perioadă de transformări majore prin care a trecut România, anume prima jumătate a secolului XX.

Domeniul „de nişă" abordat este analizat şi prezentat într-o manieră comprehensivă, volumul fiind structurat în două secţiuni complementare. Prima dintre acestea este dedicată proceselor de transformare instituţională şi de evoluţie a cadrului legislativ care au jalonat activitatea de contraspionaj în perioada 1918 – 1945. Demersul ştiinţific a reuşit să clarifice într-o mare măsură „arhitectura" instituţională existentă în epocă pe palierul contracarării acţiunilor serviciilor secrete străine care acţionau împotriva intereselor de securitate ale ţării noastre. Aceasta în condiţiile în care cercetarea a fost îngreunată de existenţa, în primele decenii ale secolului de o multitudine de instituţii cu responsabilităţi în domeniu, de numeroasele reconfigurări ale acestora, dar şi de absenţa unor diferenţieri precise între concepte precum contraspionaj, contrainformaţii, sabotaj sau chiar terorism.

Într-o manieră nu numai profesionistă dar şi atractivă pentru cititor a fost realizată ce-a de-a doua parte a lucrării, menită să reliefeze tocmai acţiunea propriu-zisă a structurilor de contraspionaj care şi-au desfăşurat activitatea în slujba statului român. Sunt urmărite succesele dar şi anumite nereuşite inerente oricărui serviciu de informaţii, ameninţările pe care au fost obligate să le contracareze, modurile ingenioase de lucru şi metodele utilizate

de serviciile adverse şi descoperite de agenţii români în activitatea curentă, dar şi cooperarea de succes avută cu serviciile partenere.

Secţiunea este împărţită generic, pornind de la actorii statali care urmăreau să pericliteze securitatea ţării, pe trei „fronturi": frontul de est, care surprinde, detaliat, raportarea Rusiei sovietice la România interbelică şi maniera în care relaţiile dintre cele două state s-au repercutat asupra activităţii de contraspionaj; frontul de sud, conturat în jurul acţiunilor spionajului bulgar şi turc, respectiv frontul de vest, unde structurile de contraspionaj naţionale s-au confruntat cu serviciile maghiar, german, italian şi anglo-american.

Practic, nici un aspect mai mult sau mai puţin semnificativ din domeniu nu este omis în paginile lucrării, aceasta devenind, fără îndoială, un reper definitoriu în istoriografia românească a istoriei serviciilor secrete.

Recomandări de lectură:
THE JOURNAL OF INTELLIGENCE HISTORY

(prezentare de **Sorin APARASCHIVEI**)

Renumita revistă „Journal of Intelligence History”[1], publicaţie oficială a *International Intelligence History Association* (IIHA), ne prezintă în numărul 1 (volumul 17) din ianuarie 2018 următoarele articole: *British military intelligence in aid of the civil power in England and Wales*, semnat de Jon Moran; *The sensitivity of SIGINT: Sir Alfred Ewing's lecture on room 40 in 1927*, semnat de Rhodri Jeffrey-Jones; *The Konnov/Mikhailov/Bakourskii espionage crises of July-August 1947 and Vyshinskii note on Raoul Wallenberg*, semnat de Johan Matz; *Japanese intelligence and covert operations: a strategic evaluation of Fujiwara Kikan in the invasion of Malaya and Singapore*, 1941-1942, sub semnătura lui Adam Leong Kok Wey; *Politicising intelligence: what went wrong with the UK and US assessments on Iraqi WMD în 2002*, semnat de Giovanni Coletta, şi *The Gatekeepers: film, television series, and book review*, semnat de Eyal Pascovich.

Prin urmare, titluri incitante şi autori consacraţi care îndeamnă la cunoaşterea şi aprofundarea unor evenimente istorice la care au contribuit din plin şi serviciile de informaţii.

Fără intenţia de a desconsidera importanţa unuia sau a altuia dintre articolele menţionate, atragem atenţia în mod deosebit asupra celui semnat de Jon Moran, intitulat: *British military intelligence in aid of the civil power in England and Wales.* De ce? Deoarece, aici, autorul încearcă să descifreze începuturile colaborării informative desfăşurate între armata britanică şi instituţiile civil-administrative ale statului, la sfârşitul secolului al XVII-lea şi începutul secolului al XX-lea, ceea ce constituie un demers care lipseşte în istoriografia serviciilor de informaţii din România.

Potrivit lui Jon Moran, pentru a înţelege deplin constituirea structurilor moderne de intelligence trebuie acordată mai multă importanţă rolului jucat în trecut de către reprezentanţii autorităţilor civile locale, adică a primarilor, prefecţilor, subprefecţilor, notarilor, miliţiilor etc., deoarece aceşti

[1] Revistă Editată de International Intelligence History Association la Routledge Taylor & Francis Group.

funcţionari şi magistraţi locali erau principalii garanţi ai ordinii publice şi, totodată, primii depozitari ai informaţiilor ce interesau siguranţa statului.

Pentru reconstituirea mecanismul prin care se adunau informaţiile privind siguranţa statului, Jon Moran îndeamnă la studierea cu atenţie a cadrului legal al vremii care reglementa adunările publice şi modul de intervenţie a structurilor de forţă în caz de dezordine socială, răzmeriţe, mişcări anarhiste, răscoale, greve, atentate etc. Una din remarcile autorului este că britanicii nu au avut o organizaţie militară care să adune informaţii sistematic şi permanent, acest lucru fiind făcut pentru prima dată de către organele locale ale intelligence-ul civil.

Aşadar, cu speranţa că interesul pentru acest număr din *Journal of Intelligence History* a fost deja stârnit, vă dorim lectură plăcută ...

ACADEMIC FOCUS

INTELLIGENCE IN THE KNOWLEDGE SOCIETY
Bucharest, October 18-19, 2018

Intelligence in the Knowledge Society - the XXIV edition

The XXIV edition of the Intelligence in the Knowledge Society conference takes places in a highly dynamic international context, which challenges both intelligence organizations, as well as intelligence and security theorists and researchers. The hybrid nature of the current conflict, which is waged through both military and non-military means such as diplomatic, economic, cyber and information operations poses new problems for old concepts. The existence of fake news and manipulation demands that state and supra-national institutions adopt policies to counter misinformation, while intelligence agencies are forced to improve their analysis capabilities to attribute attacks which might seem uncoordinated. Furthermore, the Cambridge Analytica revelations showed, once again, the power of technology and of open source information, which, if properly processed and exploited, can represent both a useful intelligence asset and a threat to individual privacy.

The conference invites both practitioners and academics to weigh in on how intelligence, understood both as a process, as an organization and as an analytically validated product can address the current challenges. Contributions are expected to bring novel perspectives on intelligence analysis, history and theory, as well as strategic past and future developments. IKS represents a forum for conversation between academics and practitioners, where both perspectives are welcome and their inter-relations can be explored.

Topics:

1. *Patchwork quilt* or *common blanket*? Recent security developments in the European Union and beyond

While NATO remains the overarching framework for trans-Atlantic security cooperation, other bi- and multi-lateral security cooperation frameworks have also played an important role in the past decade. The Lisbon Treaty, for instance, allows for the initiation of a Permanent Structured Cooperation in the field of defense in the European Union. This has been officially operationalized in late 2017, allowing for member states who are willing to pool more of their capabilities. The EU is also becoming a hub for military cooperation, such as in the case of Operation Sophia, aimed at curbing

the arrival of illegal immigrants in the Mediterranean. Finally, bilateral and multi-lateral relations are being constantly updated and interrogated, such as in the case of the Intermarium initiative. The panel aims to explore the causes and consequences of these developments and to inquire into whether these are effects of the need to address new threats or whether they are part of the classical diplomacy tool. Furthermore, the panel looks at whether collective security remains a desirable goal or whether states are pursuing diverging interests in ensuring national security.

2. Understanding the hybridity of threat: implications for intelligence analysis

Countering hybrid threats and understanding their social, security, economic and political implications have been some of the most debated topics addressed by academics and practitioners involved in addressing hybrid warfare and its attribution. While in classical warfare, it was obvious who the aggressor was, those who employ hybrid tactics take great pains to increase deniability, even when direct military action is employed. Deniability and the confusion of the adversary are crucial especially when information operations are employed. These involve the creation and anonymous distribution of fake or misleading information which supports narratives aimed to subvert social support for the legitimate government and for a country's security policy.

Furthermore, given the complex nature of the tactics, designing appropriate responses is problematic since the adversary might employ proxies or cover his action with a set of media falsehoods.

In this context, intelligence analysts are hard pressed to tell truth from fiction and real intentions from strategic dissimulation. This panel aims to inquire into how the analyst is to tackle with: coordination between enemy actions, how to separate fake news from real events, how to become efficient in early warning, integration of technological innovation and multiple source exploitation.

3. Intelligence history - recurring patterns or new dynamics?

Current developments of the international security environment show, once again, that history is a cyclical process and that defining aspects of the previous century become relevant again. The normalization of power politics in inter-state relations, the reshaping of the global power relations, regional and international tremors caused by the clash of economic and security interests of old and new state and supra-national actors remind us of defining moments in the XX century.

The panel aims to debate defining action patterns in international relations from the perspective of intelligence studies, crucial moments, including those in the „secret war" which led to today's developments. The panel thus represents a look over what is novel and what has been resurrected of the past.

4. Thinking and acting strategically in the age of uncertainty: what role for practitioners and academics in the process?

The dialogue between practitioners, experts, academics and policy makers has in the past decade proven difficult to engage and maintain, either due to the very different professional jargons or to the different outcomes they employ. In the field of strategic studies this problem has been particularly acute. While, academics aim to build models to understand the world, practitioners and experts desire to obtain an immediate solution to concrete problems and policy makers focus on identifying the right framework for the design and implementation of long term policy oriented architectures. In drafting strategic documents, professional categories should systematically engage in dialogue, with academics bringing theories, innovations and conceptual frameworks to the table, practitioners and experts identifying and evaluating the everyday problems that are to be addressed, and policy makers providing structural solutions for their implementation. With this aim in mind, this panel is meant to provide academics, experts, practitioners and policy makers with the right framework in which to debate on ardent problems they need to tackle mechanisms of cooperation

5. Security and freedom - contemporary European policies and future perspectives

The seemingly perpetual question of how to balance security and freedom has been given constantly different answers over the recent period. In the preamble of the European Security Agenda, the European Commission gives priority to fundamental rights and to the exercise of democratic accountability and control by national parliaments. At the same time, the actions it foresees represent a powerful move towards security: the strengthening of the European-wide databases such as: the Schengen Information System, the improvement of the Prüm framework and the implementation of the Passenger Name Record Directive. Conversely, through the *Digital Rights Ireland* and the *Tele2 Sverige* Decisions, the European Court of Justice has censured this view, and reminded Europeans that not all forms of data collection and processing respect fundamental rights. The panel looks for both empirical and theoretical papers outlining the debate and possible solutions for the dilemma of how to create security while maintaining individual liberty.

6. Intelligence theory – implications of contemporary developments on an old debate

Paradoxically, theory building in intelligence studies has been an area where a significant amount of work has been produced but little common ground has been found. Initially, intelligence theorizing belonged to practitioners, such as Michael Warner who debated among themselves on the meaning of the term. Within the next generation, the debate began to include academic language and theories, such as in the work of Stephen Marrin, who asked for a new conceptualization of the relationship between intelligence producers and intelligence consumers. Alternatively, Hamilton Bean, recommends the use of critical/postmodern theories to understand relations between the representation of intelligence and societal attitudes towards intelligence institutions. Finally, Jules Gaspard argues that a unitary theory of intelligence cannot be achieved since each author uses the term with a very different meaning and that "no essence" can be detected to the concept.

The panel invites authors to reflect on these issues and to criticize existing approaches in the field of intelligence theory building. Purely theoretical papers are encouraged, but also those reflecting on the impact of specific practices and overall theories are welcome.

* * *

Within this context, the "Mihai Viteazul" National Intelligence Academy invites both scholars and practitioners to submit paper abstracts for the 24th edition of its annual international conference ***Intelligence in the Knowledge Society.*** The conference will take place in **Bucharest, Romania, on 17-19 October 2018**.

Those interested in participating are invited to submit the title and summary of their proposed presentation (abstracts of maximum 300 words) by **July 30th, 2018** at intelligenceconference@sri.ro. Acceptance notifications will be sent by **August 10th, 2018**, while final papers must be submitted by **September 25th, 2018.** In addition to requesting **no registration fee,** best papers will be selected for publication in the ***Romanian Intelligence Studies Review (RRSI)***.

Author guidelines and other organisational details can be accessed on the conference website – www.iksconference.ro and further inquiries can be addressed to Mr. Valentin Nicula, conference chair – email: intelligenceconference@sri.ro.

ROMANIAN INTELLIGENCE STUDIES REVIEW
Call for paper

Mihai Viteazul` National Intelligence Academy, via its National Institute for Intelligence Studies, publishes the *Romanian Intelligence Studies Review* (RISR), a high quality peer reviewed and indexed research journal, **edited in Romanian and English twice a year.**

The aim of the journal is to create a framework for debate and to provide a platform accessible to researchers, academicians, professional, practitioners and PhD students to share knowledge in the form of high quality empirical and theoretical original research papers, case studies, conceptual framework, analytical and simulation models, literature reviews and book review within security and intelligence studies and convergent scientific areas.

Topics of interest include but are not limited to:

- Security paradigms in the 21st century
- International security environment
- Security strategies and policies
- Security Culture and public diplomacy
- Intelligence in the 21st century
- Intelligence Analysis
- Open Source Intelligence (OSINT)
- History and memory in Intelligence

Review Process: RISR shall not accept or publish manuscripts without prior peer review. Material which has been previously copyrighted, published, or accepted for publication will not be considered for publication in the journal. There shall be a review process of manuscripts by one or more independent referees who are conversant in the pertinent subject area. Articles will be selected based on their relevance to the journal's theme, originality and scientific correctness, as well as observance of the publication's norms. The editor evaluates the recommendation and notifies the author of the manuscript status.

The review process takes maximum three weeks, the acceptance or reject notification being transmitted via email within 5 weeks from the date of manuscript submission.

Date of Publishing: RISR is inviting papers for No. 21 and 22 and which is scheduled to be published on June and December, 2019.

Submission deadlines: February 1st and July 1st

Author Guidelines: Author(s) should follow the latest edition of APA style in referencing. Please visit www.apastyle.org to learn more about APA style, and http://www.animv.ro for author guidelines.

Contact: Authors interested in publishing their paper in RISR are kindly invited to submit their **proposals electronically in .doc/docx format at our e-mail address rrsi@sri.ro, with the subject title: RRSI article proposal.**

Invited reviewers:

Sorin APARASCHIVEI
- Researcher at the National Institute for Intelligence Studies, Romania

Deagoș ARDELEANU
- Lecturer, "Mihai Viteazul" National Intelligence Academy, Romania

Irena CHIRU
- Professor at "Mihai Viteazul" National Intelligence Academy, Romania

Constantin DEGERATU
- Professor at „Dimitrie Cantemir" Christian University, Romania

Florentina HĂHĂIANU
- Lecturer, "Mihai Viteazul" National Intelligence Academy, Romania

Cristina IVAN
- Researcher at the National Institute for Intelligence Studies, Romania

Ioan Codruț LUCINESCU
- Researcher at the National Institute for Intelligence Studies, Romania

Sergiu MEDAR
- Professor at „Lucian Blaga" University from Sibiu, Romania

Veronica MIHALACHE
- Associate Professor at "Mihai Viteazul" National Intelligence Academy, Romania

Cristian NIȚĂ
- Associate Professor at "Mihai Viteazul" National Intelligence Academy, Romania

Valentin STOIAN
- Researcher at the National Institute for Intelligence Studies, Romania

Bogdan Alexandru TEODOR
- Lecturer, "Mihai Viteazul" National Intelligence Academy, Romania

Iulian MARTIN
- Professor at „Carol I" National Defence Academy, Romania