CURRENT CHALLENGES AND TRENDS IN INTELLIGENCE

Ahmet ATEŞ[*]

Abstract

After a thorough examination of current intelligence literature, a variety of national security documents and respected news outlets, I find several current challenges in intelligence under different areas. I classify current major challenges in intelligence into four groups. These are technological, financial, organizational, and political. Technological challenges are the most important ones because other challenges are either related to it or a result of it. These are the expansion of using meta-data, the expansion of social media, and cybersecurity. The second current challenge in intelligence is financial. It is mostly about the use of cryptocurrencies. The third challenge is organizational. These are the impact on information revolution on intelligence organizations and competition with non-intelligence organizations. The last current challenge in intelligence is political. Political challenges are populist nationalist movements, ISIS returnees, and expansion of hybrid warfare. Related to current challenges in intelligence and the global security environment, there are eight current trends in intelligence. Five of them are mostly related to technological challenges, while three of them are related to political challenges. The trends that are related to technological challenges in intelligence are the foundation of cyber intelligence divisions/agencies, the change in recruitment policies, the rising importance of the security of cyberinfrastructure, privatization of intelligence, and increasing role of open-source intelligence. The trends that are related to political challenges in intelligence are the increasing focus on right-wing groups, the elimination of ISIS returnees, and the increasing role of intelligence in hybrid warfare/covert operations.

Keywords: *Intelligence, National Security, Cyber Intelligence, Technology*

İSTİHBARATTA GÜNCEL ZORLUKLAR VE AKIMLAR

Öz

Bu çalışmada; mevcut istihbarat literatürü, çeşitli ulusal güvenlik dokümanları ve saygın haber kaynaklarının kapsamlı incelenmesi sonucu, istihbarat alanındaki farklı güncel zorluklar bulunmuştur. Güncel zorluklar dört farklı başlık altında incelenmiştir. Bu başlıklar "teknolojik, finansal, kurumsal ve siyasal zorluklar" olarak tanımlanmıştır. Diğer zorlukların ilintili veya sonucu sebebiyle olmasından dolayı teknolojik zorlukların en önemli grup olduğu savunulmuştur. Meta-veri ve sosyal medya kullanımının artması ve siber güvenlik teknolojik zorlukları oluşturmaktadır. İkinci güncel zorluk olarak finansal zorluk tanımlanmıştır ve bu alandaki sorunun büyük oranda kripto paraların kullanımı ile ilgili olduğu savunulmuştur. Üçüncü güncel zorluğun kurumsal olduğu belirtilmiş ve temelde bilgi devrimi ve ulus-dışı istihbarat kuruluşları ile yaşanan rekabetin bu zorluğu oluşturduğu savunulmuştur. Son güncel zorluk olarak popülist milliyetçi hareketler, IŞİD'in yenilmesi sonrası ülkelerine geri dönen üyeleri ve hibrit savaşın yaygınlaşmasının siyasal zorlukları oluşturduğu savunulmuştur. Bahsedilen güncel zorluklar ve küresel güvenlik parametreleri ışığında sekiz adet güncel istihbarat akımı olduğu belirtilmiştir. Bu akımların beş tanesi teknolojik zorluklar ile ilgili iken üç tanesi siyasal zorluklar ile ilgilidir. Teknolojik zorluklar ile ilgili olan güncel istihbarat akımları siber istihbarat birimlerinin kurulması, işe alım politikalarının değişmesi, siber altyapının artan önemi, istihbaratın özelleşmesi ve açık kaynak istihbaratının artan rolü olarak belirlenmiştir. Siyasal zorluklar ile ilgili olan akımlar ise milliyetçi gruplar üzerine yapılan istihbarat faaliyetlerinin artması, ülkelerine dönen/dönmekte IŞİD üyelerinin etkisiz hale getirilmesi ve istihbaratın hibrit savaş ve örtülü operasyonlarda rolünün artması olarak belirlenmiştir.

Anahtar Kelimeler: *İstihbarat, Ulusal Güvenlik, Siber İstihbarat, Teknoloji*

[*] Ph.D. Candidate, University of Delaware, ates@udel.edu, Orcid.org/0000-0001-5184-7701

Makale Geliş Tarihi: 17.01.2020 Makale Kabul Tarihi: 03.03.2020

INTRODUCTION

In *Dr. No*, the first movie of the long series, British Royal Secret Service agent James Bond went to Jamaica and chased *Dr. No* to prevent his attack on an American space launch. In the twenty-fourth movie of the series released in 2015, James Bond fight against a global terrorist organization called Spectre. From the first movie to the last one, James Bond underwent significant changes regarding the issues that James Bond deals with. From a regular Cold War spy that focuses on the Soviets, James Bond transformed into an agent that chases transnational terrorist organizations. As in the James Bond movies, the challenges in intelligence have been rapidly changing. Consequently, trends in intelligence also have been changing. There are new strategic threats, actors, challenges, and trends in intelligence. To analyze the current international security environment more efficiently, I argue that it is essential to explore current challenges and trends in intelligence since they determine the national security settings of countries.

In this article, I aim to explore major current challenges and trends in intelligence. I classified current challenges in intelligence into four groups: a) technological, b) financial, c) organizational, and d) political. More specifically, I argue that the increasing use of meta-data, social media and cybersecurity are current technological challenges in intelligence. Likewise, the increasing use of virtual currencies is a financial challenge in intelligence, while increasing competition with the private sector is an organizational challenge. Lastly, increasing nationalism and anarchism, ISIS returnees, and expansion of hybrid warfare are political challenges in intelligence. It is important to note that the impact of these challenges may vary for different countries. However, these challenges pose a threat to all of a country's official intelligence structures to some degree regardless of the level of development of a country. The current trends, on the other hand, also are related to these challenges above. These are a) the establishment of cyber divisions within intelligence communities, b) recruiting IT-oriented personnel, c) paying more attention to cyber infrastructure, d) privatization of intelligence e) increasing role of open source intelligence, f) focusing more on right-wing groups, h) ISIS returnees and i) increasing role of intelligence in hybrid warfare/covert operations.

1. PREVIOUS STUDIES IN THE FIELD

Before providing the major current challenges and trends in detail, it is important to assess the relevant literature and discuss this article's contribution to the field. As a result of the secret nature of intelligence and because of the lack of access to

reliable data, intelligence research is one of the understudied disciplines in political science literature. Even though there were remarkable researches, mostly from Western scholars, in the field, intelligence organizations were usually examined under other disciplines such as history studies, organizational studies until the early 2000s. These studies can be grouped under three main themes: historical research, organizational research, and reform studies.

In the historical research group, the main themes in the discipline are either exploring the role of intelligence organizations in the decision-making process or the evolution of specific intelligence organizations through historical documentation. For instance, Madiera (2003), O'Halpin (2005), and Perlman (2018) examine the role of British and American intelligence organizations in the decision-making processes during the two world wars. Unlike Madiera, O'Halpin, and Perlman, other scholars such as Warner and McDonald (2005), McNeil (2008), and Jeffreys-Jones (2010) focus more on the evolution of US intelligence organizations.

In the organizational studies, the main themes in the discipline are organizational research, oversight research, and organizational culture studies. In the first theme, the main focus is exploring the internal organizational structure of intelligence organizations and its effect on intelligence conduct. For instance, Robarge (2010) examines the effect of leadership on the CIA operations while Lederman (2005) and Stimson and Habeck (2016) focus more on structural weaknesses of the US intelligence organizations. In the second theme, the main concern is the accountability of intelligence organizations and oversight processes. For instance, Farson and Whitaker (2010), Hastedt (2010), and Gill (2012) evaluate Canadian and American intelligence oversight processes. In the last theme, on the other hand, the main analysis covers the organizational cultures of specific intelligence organizations. For instance, Lahneman (2010), Boardman (2006), Davies (2004) and Best Jr. (2014) investigate how organizational culture of several US intelligence organizations affect the intelligence conduct.

Lastly, in the reform studies, researchers point to intelligence failures and reforms. For instance, while Zegart (2005; 2006), Firester (2011), and Garicano and Posner (2005) examine the causes of severe intelligence failures such as 9/11, Bruijn (2006), Nicander (2011), Smith (2004) and Rovner and Long (2005) evaluate the intelligence reform which occurred after the same intelligence failure, 9/11.

As it is briefly provided above, intelligence studies literature, mostly, do not have an academic interest to understand current challenges that intelligence organizations encounter and current trends that they follow. There are several pieces of research that tried to analyze the relatively current phenomenon, though. For instance, Warner (2012), Hansen (2014), Brantly (2018), and Regens (2019) tried to uncover the effects of the technological revolution to intelligence organizations. However, even though these studies uncover the specific portions of the current challenges, they are inadequate to provide a more comprehensive understanding of current challenges and trends in intelligence. Hence, it is vital to provide an overarching approach to understand current intelligence issues. In that regard, this article will not only fill the gap in the literature with examining several aspects of current challenges and trends in intelligence, such as political and financial, but also will be fruitful for policymakers in the current dynamic security environment.

2. CURRENT CHALLENGES IN INTELLIGENCE

As mentioned above, there are four different types of current challenges in intelligence. However, I argue that technological challenges are the most important ones since the other types of challenges are either related to them or are a result of them.

2.1 Current Technologic Challenges in Intelligence

Increasing use of meta-data: In its simplest form, metadata is the data about the data. Per Lim (2016: 627), the use of meta-data can help not only to analyze general trends or anomalies but also to improve intelligence hypotheses and to analyze massive amounts of data simultaneously. In that manner, the use of meta-data is a double-edged sword. While it can help to improve intelligence analysis of a country, it also poses a threat to the same country as well. It is also important to note that the use of meta-data leads to different types of challenges for different countries. For a technologically advanced country such as the United States, it is a handy toolbox for intelligence organizations to support policymaking. However, since no nation itself has authority over the meta-data, it can also be used by rival countries' intelligence organizations as well. In other words, while it enhances the capacity of intelligence organizations of a country, the use of meta-data by a rival country also reduces the same capacity.

Besides, technologically advanced countries, the use of meta-data poses two challenges to developing countries. On the one hand, the use of meta-data puts

developing countries' intelligence organizations in a disadvantaged position against advanced countries since they mostly rely on traditional intelligence methods. On the other hand, it highlights a need for the transformation of intelligence tools of developing countries. To transform developing countries' intelligence tools to be compatible with meta-data, these countries must invest in new technologies and recruit more IT-oriented personnel. However, most of these countries lack financial and human resources to achieve this transformation. For instance, while US intelligence organizations mostly provided more accurate intelligence analysis during the Arab Spring, Egyptian intelligence suffered providing reliable intelligence to policymakers because of the lack of the equipment and personnel that are compatible with meta-data.

The use of meta-data by non-state actors also poses a challenge to intelligence organizations. On the one hand, global terrorist organizations such as Al-Qaeda or ISIS can attract or recruit persons with high skills in technology and can enhance their capacity, find vulnerable targets and conduct attacks other than traditional methods by using meta-data. On the other hand, the private sector's use of meta-data creates competition and risk for state intelligence organizations. For instance, a private intelligence company, Black Hawk Intelligence, offers meta-data services. While state intelligence organizations need to compete with these private organizations, they also do not have any control over the services private companies provide or their customer selection.

Increasing use of social media: The importance of social media has dramatically increased in the last decade. Per Chaffey (2017), there are 3.773 billion internet users, and 2.789 billion of them actively use social media platforms. Among social media platforms, Facebook (1.871 billion active users), WhatsApp (1 billion active users), Instagram (600 million active users), and Twitter (317 million active users) are the most popular ones (Chaffey, 2017; Libo-on, 2016). In other words, approximately forty-five percent of the total world population are active social media users. Heavily use of social media poses, at least, three challenges to intelligence organizations: a) its impact on the decision-making process, b) use of non-state actors, and c) use of encrypted messaging applications. The increasing role of traditional media's social media accounts and the very social media create a competition for state intelligence institutions regarding policy attention that brings a dilemma for intelligence professionals (Rovner, 2013: 264). On the one hand, if intelligence organizations continue with traditional methods of intelligence gathering, they may be left behind the social media information circle. However, on the other hand, if they lose their institutional standards, their

credibility may vanish (Rovner, 2013: 264). In that manner, either they may be irrelevant or outdated, or they lose their credibility while trying to catch up with the speed of social media platforms (Rovner, 2013: 267-268). Also, as Walsh (2017: 442) points, the use of social media not only decreased public trust in intelligence organizations but also the trust of the policymakers.

Another challenge related to the increasing use of social media is its use of non-state actors. Because of social media platforms, terrorist organizations can deliver their message to a broader audience and can use these platforms as recruitment tools. Currently, terrorist organizations upload terrorist contents such as statements and beheadings to these platforms and reach a global audience (Cozine, 2016: 3). Several terrorist organizations use these platforms operational and share content, such as instructions/directions of conducting a terrorist attack. In addition to reaching a broader audience, terrorist organizations also use social media platforms heavily to recruit new members. For instance, ISIS attracted more than 20.000 English-language followers only on Twitter (Committee on Homeland Security, September 2015: 6 quoted in Cozine, 2016: 4). Not only ISIS but also other terrorist organizations such as Al-Qaeda and Boko-Haram also benefit social media platforms for both propaganda and recruitment (Committee on Homeland Security, May 2017: 6-7). In addition to propaganda and recruitment, social media platforms are also used by terrorist organizations to spread new methods of terrorist attacks. For instance, after ISIS' declared on social media that its sympathizers or followers could conduct jihad with anything instead of finding weapon and arms, there were 14 attacks that a vehicle was used as a weapon and 44 attacks that edged weapons used as a weapon between 2013 and 2017 (Committee on Homeland Security, Terror Threat Snap Shot, 2017:1). As can be seen in these examples, the expansion of social media is a vital challenge for intelligence organizations. On the one hand, intelligence organizations must cope up with terrorism in this very new area, which is different than traditional methods of chasing terrorists as a result of anonymity and needs specific skills and recruitment. On the other hand, intelligence organizations also should provide counter-messaging on social media as well. In other words, even though the struggle between intelligence agencies and terrorist organizations remains, it is now happening on a different stage.

Related to the expansion of social media, another current technological challenge in intelligence is encrypted messaging applications such as WhatsApp or WeChat. Since they allow secrecy in their very nature, it is being used by terrorists for communication, organizing and conducting terrorist attacks. For instance, an ISIS-linked Afghan refugee, Riaz Khan, in Germany injured four people by

attacking them with an axe on 19th July 2016 (BBC, July 16, 2016). According to Moore (2017), ISIS encouraged and guided Riaz Khan before and during the attack through WhatsApp. As in social media, the expansion of encrypted messaging applications is a technological challenge to intelligence organizations. To counter this type of threat and prevent terrorist attacks that are planned through encrypted messaging applications, intelligence organizations also need to acquire new technologies and recruit IT-oriented people. It is also important to keep in mind that besides the social media and encrypted communication applications, the internet itself poses a challenge to intelligence communities as well because it is an ideal network for terrorist capabilities that terrorists can exchange information and can conduct anonymous and costless internet search for potential targets (Heidenreich and Gray, 2014: 18-20).

Cybersecurity issues: Regarding cybersecurity, there are two major challenges for intelligence organizations: a) anonymity and b) cyber intelligence issues. Cybersecurity is vital for intelligence organizations to protect their respected countries against traditional and non-state threats. However, the anonymity of the cyber domain creates a challenge for intelligence organizations. On the one hand, since it is almost impossible to prove to track a cyber-attack and, therefore, to provide a reciprocal response, it is a vital problem regarding deterrence. On the other hand, cyber-attacks conducted by terrorist organizations are much harder to detect and disrupt beforehand than conventional terrorist attacks. Another important aspect of cyber issues is strictly related to conducting cyber intelligence operations. As in traditional intelligence conduct, cyber intelligence also seeks to fully analyze all aspects of the threat, such as uncovering perpetrators and possible actions for the future (Mattern et al., 2014: 704). However, because of the nature of the cyber domain, identifying a threat, collecting and analyzing information, and preventing a cyber-attack is not similar to traditional methods of intelligence. Therefore, it poses a challenge to intelligence organizations. Also, the timing and complexity of cyber-attacks led to a more difficult task for intelligence organizations. Per Wirtz (2017: 762), since a warning of a cyber-attack, if any, can be received between seconds and a couple of days, the options for threat assessment and choosing the relevant response is extremely limited. Similarly, because of the complexity of the attacks in the cyber domain, assessing the complexity and providing a decent response is significantly hard for intelligence organizations (Wirtz, 2017: 762).

In addition to these two challenges, it is also important to bear in mind that cybersecurity is one of the harshest areas that state intelligence institutions and

private sector compete. Per Degaut (2016: 510), the increasing importance of the cyber domain already created tension between intelligence professionals and the private sector. Since cybersecurity requires a variety of specific skills and personnel, the private sector in several countries is eager to take part in cybersecurity and therefore receive additional funds. To compete with the private sector, state intelligence organizations must transform themselves not to be outdated, not to lose their credibility, their role in the policymaking process, and funding from the governments.

As discussed above, technological advancements brought several challenges to intelligence organizations. It is important to stress that all these technological challenges are related to one another. Together, they challenge intelligence organizations to acquire new technologies, adopt new methods, and change their recruitment policy regardless of the development level or the regime type of a country.

2.2 Current Financial Challenges in Intelligence

Countering terrorist financing is one of the most important areas of financial intelligence, and it especially became crucial for intelligence organizations after 9/11. Since terrorists need financing to planning and conducting attacks and recruitment (Rudner, 2006: 35), countering terrorist financing is vital for counterterrorism intelligence. Not only intelligence officials but also academia (Gilmore, 2004; Biersteker and Eckert, 2007; Shehu, 2012; Cooper, 2014; Ryder, 2015) extensively researched the traditional methods of terrorist financing such as the Hawala system. Likewise, international organizations such as the Financial Actions Task Force (FATF) implement several policies to counter terrorist financing. Currently, terrorist financing is not a major challenge anymore for intelligence organizations, thanks to the work of both intelligence officials and academia. However, related to technological advancements, I argue that there is a new challenge in intelligence regarding terrorist financing: virtual currencies.

There are multiple virtual currencies, but the most used one is Bitcoin. It was invented in 2009 by an unknown group called themselves Satoshi Nakamoto (Davis, 2011). It can be moved anonymously, and it is out of government regulation (Turpin, 2014: 337). Since it allows anonymity and it is not under government regulation, it became an appealing way of terrorist financing. For instance, Hamas and its armed wing, the Qassam Brigades, and ISIS started to use cryptocurrencies to finance their activities (Popper, 2019; Dion-Schwarz et al.,

2019: 8-9; SM Irwin et al., 2014: 62). Tu and Meredith (2015: 330) and Vovchenko (2017) also stressed the current financial regulations are not adequate and inappropriate for Bitcoin and cryptocurrencies are national security threats. Consequently, the use of cryptocurrencies in terrorist financing led to a crucial challenge for intelligence organizations. On the one hand, in addition to terrorist financing, terrorist organizations can also use cryptocurrencies to disrupt the sovereignty of the targeted country and increase their political and economic power (Baron et al., 2015: x). On the other hand, since some of the terrorist organizations may not have required sophisticated cyber skills, rogue states may offer its assistance to terrorist organizations in that manner (Baron et al., 2015: xi). Therefore, intelligence organizations need to uncover this kind of relationship between nation-states and terrorist or proxy groups.

Besides terrorist financing issues, the expansion of cryptocurrencies poses another threat to developing countries' intelligence organizations. In order to compete with advanced countries' intelligence organizations and to counter financial threats more effectively, developing countries' intelligence organizations need to invest in technological infrastructure and recruit financial and IT-oriented personnel. Given the lack of required funds and personnel, this challenge will likely to continue to disrupt these intelligence organizations' intelligence conduct.

In sum, regardless of the level of development of a country, all state intelligence organizations must deal with the expansion of cryptocurrencies and its use on terrorist financing. To do it adequately, intelligence organizations need to transform themselves, their strategies, and recruitment policies.

2.3 Current Organizational Challenges in Intelligence

In addition to current technological and financial challenges, there are also organizational challenges for intelligence organizations as well. These challenges can be grouped into three domains: compartmentalization issues, hierarchy issues, and competition issues. It is also important to keep in mind that most of these organizational challenges are also strictly related to technological advancements.

Compartmentalization issues: Recent technological advancements started to have a vital impact on the intelligence analysis workflow, skills, and organization (Hare and Coghill, 2016: 857). The variety and the amount of data that intelligence personnel analyze dramatically increased in the last decade. Also, the increasing use of technical tools to filter and categorize the massive amount of data (Hare and Coghill, 2016: 863), force analysis, and technical units of intelligence

organizations to fully cooperate in providing more reliable and timely intelligence to policymakers. Therefore, compartmentalization of the information, which is a norm in intelligence organizations, creates an organizational challenge to intelligence organizations. If intelligence organizations start to relax compartmentalization in their workflow, then they face information security problems.

Hierarchy issues: Intelligence organizations are strict hierarchies by their nature. However, with the expansion of open-source data and the complexity of the current security problems, strict hierarchies may not be useful anymore. To understand current security challenges and to enhance their capability to counter current threats, intelligence organizations need to update their organizational structure and should be more loosely networked, more collaborative, and less hierarchical such as private companies like Google or Facebook (Hare and Coghill, 2016: 870). Considering bureaucracies are usually resistant to radical changes, and transformational changes occur exceptionally rare, this transformation stays as another current organizational challenge for intelligence organizations.

Competition issues: The growing influence and role of private intelligence organizations, think tanks, and media outlets in policymaking processes not only led to privatization of intelligence but also pose a challenge to state intelligence organizations, which have long been the only legitimate source of information for policymakers (Denécé, 2014: 36). Even though privatization of intelligence started in the 1980s and boosted after the end of the Cold War (Matey, 2013: 278), with the recent technological advancements, private intelligence organizations became more important actors in the global security environment in the last decade. On the one hand, state intelligence organizations are having problems recruiting high-skilled personnel since private intelligence organizations also offer better opportunities. On the other hand, the transfer of experienced intelligence personnel to the private sector poses a human source management problem for state intelligence organizations.

Not only private intelligence companies but also several international NGOs and think tanks also conduct intelligence activities. For instance, Human Rights Watch as a policy-oriented advocacy NGO and RAND as a think tank provide intelligence products to policymakers and the public as well (Gentry, 2016: 477-485). In that manner, on the one hand, state intelligence organizations must compete with their counterparts as they have been doing for centuries in different forms. On the other hand, they also need to compete with non-state intelligence

organizations such as private intelligence organizations, NGOs and think tanks. In a dynamic security environment with a huge amount of data and several actors, state intelligence organizations may fail to deliver timely and accurate intelligence to policymakers. In that scenario, policymakers may choose to receive intelligence from other actors over time, which is a risk for state intelligence organizations to be irrelevant or outdated. Therefore, state intelligence organizations must transform themselves to compete in a harsher environment.

2.4 Current Political Challenges in Intelligence

Among others, there are three current major political challenges for intelligence organizations: the rising activities of the radical left and right movements as a result of populism, ISIS returnees as a result of the dissolution of ISIS, and expansion of hybrid warfare.

Rising activities of radical left and right: As a political movement, neither nationalism nor anarchism is new. However, with the increase of populism and the expansion of social media, the dissemination of propaganda and the organizing of a nationalist or anarchist movement has become relatively easier. Populist nationalism varies in different countries. For instance, it can be easily observed that populist nationalism in the United States of America contains racist motives such as white supremacy, while it is more likely to contain Islamophobia in continental Europe. Even though these movements are subject to sociological examination, it also became a subject of intelligence organizations because it poses a threat to national security. It is also important to stress why these movements constitute a challenge to intelligence organizations. For instance, after 9/11, most Western intelligence organizations' priority became Radical Islamic terrorism. Therefore, these organizations allocated most of their resources and assets to counter this threat. However, people who involve these populist movements, whether nationalist or anarchist, are mostly middle-class and were not perceived as a threat before (Struyk, 2017). In that manner, it is a must and a challenge for intelligence organizations to reorganize their threat and analysis priorities, methods, and resources in the light of rising nationalism and anarchism.

ISIS returnees: The second political challenge is strictly related to ISIS. Unlike previous transnational terrorist organizations such as Al-Qaeda, ISIS became a pseudo-state between 2014 and 2017. On the one hand, ISIS controlled more than 34.000 square miles in Syria and Iraq that shrunk to 23.320 at the end of 2016 (CNN, 2017). On the other hand, and more importantly, ISIS had 100.000 fighters

at its peak, and 15.000 of the fighters are not from the region and joined ISIS from 80 different countries (Gartenstein-Ross, 2015; Cronin, 2015). After the defeat of ISIS in late 2017, ISIS members from the different countries started to return their countries. Since it is mostly intelligence organizations' responsibility to evaluate and provide an adequate response to counter ISIS returnees, it s argued that it is still a significant political challenge for intelligence organizations.

Expansion of hybrid warfare: Unlike conventional warfare, hybrid warfare contains not only the utilization of military assets but also other several elements, including cyber and paramilitary. This type of warfare not only requires high-level intelligence coordination and personnel with different skill sets but also have severe political consequences/outcomes. Russian operations in Crimea, East Ukraine, and Syria brought not only intelligence professionals' but also public attention to this concept (Fabian, 2019: 308; Renz, 2016: 283). Therefore, the use of hybrid methods in warfare brought a challenge to intelligence organizations. On the one hand, intelligence organizations need to update their intelligence tradecraft to conduct this type of warfare. On the other hand, and more importantly, intelligence organizations must develop policies/strategies to counter hybrid threats, disrupt rival hybrid operations, and reduce the political effects of hybrid warfare. Hence, I argue that the expansion of hybrid warfare is a current political challenge for intelligence organizations.

Table-1. Current Challenges in Intelligence

CURRENT CHALLENGES IN INTELLIGENCE			
TECHNOLOGICAL	**FINANCIAL**	**ORGANIZATIONAL**	**POLITICAL**
Increasing use of meta-data	Cryptocurrencies and terrorist financing	Compartmentalization issues	Rising activities of radical left and right.
Increasing use of social media		Hierarchy issues	ISIS returnees
Cybersecurity issues		Competition issues	Expansion of hybrid warfare

Given the major current challenges in intelligence in detail, I turn my focus to current trends in intelligence. In the rest of the paper, I examine the trends in detail. It is important to note that most of the current trends in intelligence are state intelligence organizations' efforts to counter these challenges above. Intelligence

organizations are usually successful in integrating new security environment as a result of these challenges. However, it is still an ongoing process, and some organizations may be inadequate in following the trends in intelligence.

3. CURRENT TRENDS IN INTELLIGENCE

It is fair to argue that all the current trends in intelligence are mostly related to technological challenges. The main motivation behind these trends is to reorganize intelligence organizations in line with technological advancements. Therefore, intelligence organizations may solve other challenges/problems as well, such as organizational challenges. Related to technological challenges in intelligence, there are five trends. The first is the foundation of cyber divisions within intelligence organizations for those they do not already have. For those who have cyber divisions, the trend is the rising importance of this kind of division in organizations and decision-making levels.

As I briefly mention above, most of the intelligence agencies now have cyber divisions, unlike the early 2000s. Even though the CIA, US external intelligence agency, have had the Directorate of Science and Technology more than fifty years (CIA, 2007), it founded a new directorate, the Directorate of Digital Innovation, specifically focusing on cyber-related issues in 2015 (CIA, 2015; Taylor, 2015). The FBI, US domestic intelligence agency, on the other hand, founded its cyber division much earlier than the CIA. The FBI Cyber Division was founded in 2002 (FBI, 2003), but its role and importance in the decision-making process boosted in the late 2000s (FBI, 2016). Another example is Turkey. Even though the main Turkish Intelligence Agency, which is responsible for both internal and external intelligence, the MIT (The National Intelligence Organization – Milli Istihbarat Teskilati in Turkish) was founded in 1965 (MIT), its cyber branch was founded in 2016 (Tremblay, 2016). Also, the Government Communications Headquarters (GCHQ), British technical intelligence agency, was founded in 1911, creating a new division that only focuses on cyber issues, National Cyber Security Centre, in 2016 (NCSC, 2017). As we see in the examples from different countries, the creation of a cyber division within intelligence agencies to tackle the technological challenge is a current trend in intelligence.

Not only cyber divisions within intelligence organizations but also inter-agency platforms were founded in response to technological challenges. For instance, the U.S. Cyber Threat Intelligence Integration Center is one of them. As a multiagency platform, it was founded in 2015 to integrate the US intelligence community in

technology-related issues (CTIIC, date not determined). As CTIIC, Nationales Cyber-Abwehrzentrum (The National Cyber Defense Center) was founded in Germany in 2011 to promote cooperation among German intelligence agencies in technology-related issues (Fischer and Reissmann, 2011). As we see above, as in the foundation of cyber divisions within intelligence agencies, the foundation of inter-agency platforms in cyber-issues also is a trend in intelligence.

The second general trend related to technological challenges in intelligence is the change in recruitment policies of intelligence agencies. Regardless of the country, most of the intelligence organizations now require advanced level technological skills for their prospective employees. In other words, technical knowledge became a must in recruitment policies of intelligence structures. Intelligence organizations around the world may have extraordinary recruitment processes as the nature of the job. Though I am aware of that, it is also important that they recruit in formal ways. Hence, I argue that we can observe the second trend in intelligence in their formal recruitment processes. For instance, the CIA specifically focuses on technological skills to recruit. It offers a variety of jobs related that require specific technical skills such as cyber exploitation officer, cyber threat analyst, and cybersecurity officer to employ under newly-founded the Directorate of Digital Innovation (CIA, 2009; CIA, 2016). It also emphasizes the importance of meta-data and offers positions such as data engineers and data scientists (CIA, 2009). Like the CIA, another American intelligence agency, the FBI, also puts a special emphasis on hiring technology-skilled officers. It explicitly addresses that candidates who have specific technology-related degrees such as Computer Network Analysis, Cyber Forensics, and Network engineering are preferred (FBI, date note determined). As we see in the US's most-known two intelligence organizations, there is a trend in intelligence to hire more technology-skilled personnel to tackle with current technological challenges in intelligence.

Not only US intelligence organizations but also several European intelligence organizations also follow the same trend. Bundesnachrichtendienst (BND), the external intelligence agency of Germany, also specifically seeks technology-skilled candidates such as computer scientists, information management specialists, database administrators, and system engineers (Bundesnachrichtendienst, date not determined). As German intelligence, the British intelligence seeks for technology-skilled recruits. Pointing that technology-related jobs in the British intelligence is one of the most important ones, the Secret Intelligence Service (MI6) offers positions for IT infrastructure analysts, program level system engineers, and cyber

operation specialists (Secret Intelligence Service). Another example of this trend is French Intelligence. Direction Générale de la Securite Exterieure (DGSE), the external intelligence agency of France, specifically hires technology-skilled officers under the Category B of recruitment policy (DGSE, 2017). Last but not least, the Turkish National Intelligence Organization, the MIT, also puts a special emphasis on hiring tech-skilled recruits and seeks candidates in the fields of network management, systems engineering, and data mining (MIT, date not determined). As shown in examples from different countries, it can be observed a change in recruitment policies of intelligence organizations- the second trend in intelligence related to technological advancements.

Not as easily observed as the first two trends, there is also another trend that is related to technological challenges. It is strictly related to cyberinfrastructure. More dependency on technological systems in intelligence creates more vulnerability regarding infrastructure. In that manner, some intelligence organizations started to work on this issue and that may become a trend shortly. For instance, arguing that the company may have ties with Russian-sponsored cyberespionage, the US government banned the use of Kaspersky software, a Russian brand, for all federal agencies by the directive of acting Secretary of Homeland Security Elaine Duke (Nakashima and Gillum, 2017). Likewise, British intelligence organizations, including MI5 and MI6, have banned the use of Lenovo computers for cyberespionage reasons (Milmo, 2013). It is also important to note that Lenovo is a Chinese company and accused of having links to the Chinese state (Milmo, 2013). These actions may be a trend in intelligence shortly and may produce a new challenge: having a national cyberinfrastructure.

The fourth trend related to technological challenges is the privatization of intelligence. Even though increasing the role and influence of private intelligence organizations poses a threat to the credibility of formal intelligence organizations, the volume of data to be processed and the complexity of the threats are beyond intelligence organizations' analysis and operational capabilities. Therefore, several intelligence organizations have been recently outsourcing intelligence analysis and operations to either private intelligence companies or private military companies. For instance, US intelligence organizations started to outsource most of their technical intelligence requirements to the private sector after 9/11, and the role of private companies in US intelligence analysis has been exponentially increased in the last decade (Chesterman, 2008; Singh, 2019). Likewise, it can be easily observed that Russian intelligence organizations outsource some of their

intelligence operations to private military companies such as the Wagner Group. As Marten (2019: 181) observes, the Wagner Group and its antecedents operated in Africa, Eurasia, and the Middle East on behalf of Russian intelligence organizations during the last ten years.

The last trend related to technological challenges is increasing the role/use of open-source intelligence in intelligence analysis and operations. With the expansion of technological advancements and exposure, intelligence organizations started to benefit more from open-source intelligence in the last decade. Apart from the traditional Cold War intelligence tradecraft, which mostly based on human intelligence, intelligence organizations started to use open-source intelligence techniques such as natural language processing, geo-coding network analysis, and digital forensics to increase the efficiency of intelligence conduct (Ünver, 2018: 8-13). However, it is fair to argue that increasing the use of open-source intelligence is a double-edged sword. While intelligence organizations benefit from these techniques, it also poses a threat to the integrity of human intelligence operations abroad. As a result of the increasing use of open-source intelligence techniques, it became much harder to conduct operations abroad (Lucas, 2019; McLaughlin and Dorfman, 2019).

In addition to technological challenges and trends, there are also several trends in response to current political challenges in intelligence. The first trend is increasing focus on right-wing organizations. The Department of Homeland Security is one of the intelligence agencies that started to focus on right-wing groups and seemed to start this trend. In its report in 2015, the DHS equates right-wing extremist groups to Islamic extremist groups (Howell, 2015). The FBI is another intelligence agency that follows this trend. According to its new chief, Christopher Wray, the FBI has opened 1000 investigations into potential domestic terrorists linked to right-wing and left-wing movements (Levine, 2017). As in the US, European intelligence organizations also started to focus on right-wing groups. For instance, British intelligence played a key role in arresting right-wing terrorists in 2017, and intelligence officials stressed that right-wing groups started to be treated as seriously as jihadist terrorists (Dodd and Grierson, 2017). However, it may not always be the case for all countries. For instance, the German federal intelligence agency, BfV, was accused of cooperating with right-wing groups (Deutsche Welle, 2017). Despite the German case, it can be easily said that focusing on populist nationalism movements, either right-wing or left-wing, is a current trend in intelligence.

The second trend in response to current political challenges in intelligence is to eliminate ISIS returnees before they come back to their countries. Most Western intelligence organizations have been trying to eliminate ISIS returnees before coming back to their country, considering they may cause more harm in the country if they return. The UK is the most serious actor in this trend. It is reported that British special forces were tasked to kill 200 British jihadis before they come back to the UK (Kentish, 2016). The head of British domestic intelligence, MI5, said 130 British Jihadis were already killed in October 2017 (Meredith, 2017). Also, the British international development minister, Rory Stewart, openly expressed that the only way to deal with ISIS returnees is to kill them (Meredith, 2017). According to Dyer (2017), British intelligence is not the only one who hunts down ISIS members from their country. American, Australian, and French intelligence are also working on eliminating their citizens that joined ISIS (Dyer, 2017). In other words, the current trend in intelligence related to political challenges is to eliminate ISIS returnees before they go back to their home country.

The third intelligence trend in response to current political challenges in intelligence is adapting the increasing role of intelligence in hybrid warfare/covert operations. As previously mentioned, the expansion of hybrid warfare is a political challenge to intelligence organizations, and it seems that intelligence organizations started to adapt their tradecraft to conduct a hybrid approach that includes cyber and paramilitary elements. This shift can be seen in US and Russian intelligence operations to ISIS. For instance, to counter ISIS and in addition to ground operations, US intelligence organizations not only use covert and overt strategies including setting up social media networks in several local languages to counter-messaging and implanting militant networks to mimic ISIS commanders' messages to disrupt the organization but also conduct cyber operations against a non-state threat for the first time in the US history (Bouzis, 2015: 888-889; Sanger, 2016). Likewise, to counter ISIS and to gather intelligence and in addition use of private military companies in the battleground, Russian intelligence organizations, particularly the FSB, forced/encouraged Russian citizen jihadis to join ISIS by dropping charges against local jihadis and providing them new passports (Mazurova, 2016: 5).

Last but not least, unlike the trends in technology or politics, it is hard to observe the trends in financial challenges. Since virtual currency is relatively new, and it is lack of regulation, there is not an observable trend in intelligence to counter the current financial challenges. The summary of these trends can be seen in Table 2 below.

CURRENT TRENDS IN INTELLIGENCE	
TECHNOLOGY-RELATED	**POLITICS-RELATED**
Establishment of cyber divisions and interagency platforms	Increasing focus on populist right-wing groups
Change in recruitment policies	Eliminating ISIS returnees
Cyberinfrastructure	Adapting the increasing role of intelligence in hybrid warfare/covert operations
Privatization of intelligence	
The increasing role of open-source intelligence	

Table-2. Current Trends in Intelligence

CONCLUSION

After a thorough examination of current intelligence literature, a variety of intelligence organizations' documents, and respected news outlets, I find several current challenges in intelligence under different areas. I classify current major challenges in intelligence into four groups. These are technological, financial, organizational, and political. Technological challenges are the most important ones because other challenges are either related to it or are a result of it. These are increasing use of meta-data, social media, and cyber issues. The second current challenge in intelligence is financial. It is mostly about the use of cryptocurrencies. The third challenge is organizational. These are mostly the impact on information revolution on intelligence organizations and competition with non-intelligence organizations. The last current challenge in intelligence is political. Political challenges are populist nationalist movements, ISIS returnees, and expansion of hybrid warfare.

Related to current challenges in intelligence and the global security environment, there are eight current trends in intelligence. Five of them are mostly related to technological challenges, while three of them are related to political. The trends that are related to technological challenges in intelligence are the foundation of cyber intelligence divisions/agencies, change in recruitment policies, the rising importance of cyberinfrastructure, privatization of intelligence, and increasing role of open-source intelligence. The trends that are related to political challenges in intelligence are the increasing focus on right-wing organizations, the elimination of ISIS returnees, and adapting the increasing role of intelligence in hybrid warfare/covert operations.

Understanding current challenges and trends in intelligence can help us to analyze and explain the global security environment to a greater degree. In that regard, this article should help national security scholars and intelligence professionals. It is also important to acknowledge that it is not a constant phenomenon. On the contrary, it is a dynamic process, and I argue that challenges and trends co-evolve. Future research in this area should focus on these challenges and trends closely. In doing so, researchers can offer more systematic and more insightful works that will be helpful for both the field, intelligence studies, and intelligence officials.

REFERENCES

Baron, J., O'Mahony, A., Manheim, D., Dion-Schwarz, C. (2015). *National security implications for virtual currency: Examining the potential for non-state actor deployment.* RAND. Santa Monica, United States.

BBC. (July 19, 2016). *Germany axe attack: assault on train in Wuerzburg injures HK family*. Retrieved from. http://www.bbc.com/news/world-europe-36827725 Access: 14/11/19

Best Jr, R. A. (2014). Leadership of the US Intelligence Community: From DCI to DNI. *International Journal of Intelligence and Counterintelligence*, 27(2), 253-333.

BlackHawk Intelligence (2017). Metadata Analysis. Retrieved from. http://www.blackhawkintelligence.com/corporate-services/it-forensics/it-forensics/metadata-analysis/ Access: 13/11/19

Boardman, C. H. (2006). *Organizational Culture Challenges to Interagency and Intelligence Community Communication and Interaction*. National Defense University, Norfolk VA, Joint Advanced Warfighting School.

Bouzis, K. (2015). Countering the Islamic State: US counterterrorism measures. *Studies in Conflict & Terrorism*, 38(10), 885-897.

Brantly, A. F. (2018). When everything becomes intelligence: machine learning and the connected world. *Intelligence and National Security*, 33(4), 562-573.

Bruijn, H. D. (2006). One fight, one team: the 9/11 commission report on intelligence, fragmentation and information. *Public Administration*, 84(2), 267-287.

Bundesnachrichtendienst. *Stellenanzeigen im Gehobenen Dienst*. Retrieved from. http://www.bnd.bund.de/DE/Karriere/Stellenanzeigen/Gehobener_Dienst/Stellenanzeigen_node.html Access: 22/11/19

Central Intelligence Agency. (December 19, 2016). *Cyber Operations Officer*. Retrieved from. https://www.cia.gov/careers/opportunities/support-professional/cyber-operations-officer.html Access: 22/11/19

Central Intelligence Agency. (May 5, 2007). *Science & Technology*. Retrieved from. https://www.cia.gov/offices-of-cia/science-technology 22/11/19

Central Intelligence Agency. (October 1, 2015). *Digital Innovation*. Retrieved from. https://www.cia.gov/offices-of-cia/digital-innovation 22/11/19

Central Intelligence Agency. (September 21, 2009). *Careers & Internships*. Retrieved from. https://www.cia.gov/careers/opportunities/cia-jobs Access: 22/11/19

Chaffey, D. (April 27, 2017). Global social media research summary 2017. *Smart Insights*. Retrieved from. https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/ Access: 14/11/19

Chesterman, S. (2008). We Can't Spy … If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions. *The European Journal of International Law*, 19(5), 1055-1074.

CNN (October 17, 2017). *ISIS Fast Facts*. Retrieved from. http://www.cnn.com/2014/08/08/world/isis-fast-facts/index.html Access: 24/11/19

Committee on Homeland Security, U.S. House of Representatives. (May 2017). *Terror Threat Snap Shot*. Retrieved from. file:///C:/Users/Ahmet%20Ates/Downloads/nps84-050817-04.pdf Access: 14/11/19

Committee on Homeland Security, U.S. House of Representatives. (September 2015). *Terror Threat Snap Shot*. Retrieved from. https://homeland.house.gov/wp-content/uploads/2015/09/Complete-September-Terror-Threat-Snapshot.pdf Access: 14/11/19

Cozine, K. (2016). Social Media and the Globalization of the Sicarii. *Global Security Studies*, 7(1).

Cronin, A. K. (2015). ISIS is not a terrorist group: why counterterrorism won't stop the latest jihadist threat. *Foreign Affairs*. Retrieved from. https://www.foreignaffairs.com/articles/middle-east/isis-not-terrorist-group Access: 24/11/19

Cyber Threat Intelligence Integration Center. *Who we are*. Retrieved from. https://www.dni.gov/index.php/ctiic-who-we-are Access: 22/11/19

Davies 1, P. H. (2004). Intelligence culture and intelligence failure in Britain and the United States. *Cambridge Review of International Affairs*, 17(3), 495-520.

Davis, J. (October 10, 2011). The crypto-currency: bitcoin and its mysterious inventor. *The New Yorker*. Retrieved from.

https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency Access: 19/11/19

Degaut, M. (2016) Spies and Policymakers: Intelligence in the Information Age, *Intelligence and National Security*, 31(4), 509-531.

Denécé, E. (2014). The Revolution in Intelligence Affairs: 1989–2003. *International Journal of Intelligence and Counterintelligence*, 27(1), 27-41.

Deutsche Welle. (May 17, 2017). *Reports: German intelligence recruited head of neo-Nazi group as informant*. Retrieved from. http://www.dw.com/en/reports-german-intelligence-recruited-head-of-neo-nazi-group-as-informant/a-38866369 Access: 24/11/19

Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2019). *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*. Rand Corporation, Santa Monica, United States.

Direction Générale de la Securite Exterieure. (October 10, 2017). *Categorie B*. Retrieved from. http://www.defense.gouv.fr/english/dgse/tout-le-site/categorie-b Access: 22/11/19

Dodd, V. & Grierson, J. (September 27, 2017). Eleven men arrested on terror charges in neo-Nazi investigation. *The Guardian*. Retrieved from. https://www.theguardian.com/uk-news/2017/sep/27/eleven-men-arrested-on-terror-charges-neo-nazi-investigation-national-action Access: 24/11/19

Dyer, E. (November 17, 2017). `Canada does not engage in death squads` while allies actively hunt down their own foreign fighters. *CBC News*. Retrieved from. http://www.cbc.ca/news/politics/isis-fighters-returning-target-jihadis-1.4404021 Access: 24/11/19

Fabian, S. (2019). The Russian hybrid warfare strategy–neither Russian nor strategy. *Defense & Security Analysis*, 35(3), 308-325.

Farson, S., & Whitaker, R. (2010). Accounting for the Future or the Past?: Developing Accountability and Oversight Systems to Meet Future Intelligence Needs. In *The Oxford Handbook of National Security Intelligence*, Oxford University Press, 673-681.

Federal Bureau of Investigation (July 17, 2003). *Testimony*. Retrieved from. https://archives.fbi.gov/archives/news/testimony/the-fbis-cyber-division Access: 22/11/19

Federal Bureau of Investigation (July 26, 2016). *Countering the cyber threat: New U.S. cyber security policy codifies agency roles.* Retrieved from. https://www.fbi.gov/news/stories/new-us-cyber-security-policy-codifies-agency-role Access: 22/11/19

Federal Bureau of Investigation. *Using Innovation to Protect the Nation*. Retrieved from. https://www.fbijobs.gov/career-paths/stem Access: 22/11/19

Firester, D. (2011). *Failure to adapt; Intelligence Failure and Military Failure as Functions of Strategic Failure?*, Retrieved from. https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1045&context=cc_etds_theses Access: 25/02/20

Fischer, S. & Reissmann, O. (June 16, 2011). Germany establishes new cyber defense center. *The Atlantic Council*. Retrieved from. http://www.atlanticcouncil.org/blogs/natosource/germany-establishes-new-cyber-defense-center Access: 22/11/19

Garicano, L., & Posner, R. A. (2005). Intelligence failures: An organizational economics perspective. *Journal of Economic Perspectives*, 19(4), 151-170.

Gartenstein-Ross, D. (February 9, 2015). How many fighters does the Islamic State really have?. *War on the Rocks*. Retrieved from. https://warontherocks.com/2015/02/how-many-fighters-does-the-islamic-state-really-have/ Access: 24/11/19

Gentry, J. A. (2016). Toward a Theory of Non-State Actors' Intelligence, *Intelligence and National Security*, 31(4), 465-489.

Gill, P. (2012). Intelligence, Threat, Risk and the Challenge of Oversight. *Intelligence and National Security*, 27(2), 206-222.

Hansen, M. (2014). Intelligence Contracting: On the Motivations, Interests, and Capabilities of Core Personnel Contractors in the US Intelligence Community. *Intelligence and National Security*, 29(1), 58-81.

Hare, N. & Coghill, P. (2016) The future of the intelligence analysis task, *Intelligence and National Security*, 31(6), 858-870.

Hastedt, G. (2010). The Politics of Intelligence Accountability. In *The Oxford Handbook of National Security Intelligence*, Oxford University Press, 719-734.

Heidenreich, B., & Gray, D. H. (2014). Cyber-Security: The Threat of the Internet. *Global Security Studies*, 5(1), 17-26.

Howell, K. (February 21, 2015). DHS report warns of domestic right-wing terror threat. *The Washington Times*. Retrieved from. https://www.washingtontimes.com/news/2015/feb/21/dhs-intelligence-report-warns-of-domestic-right-wi/ Access: 24/11/19

Jeffreys-Jones, R. (2010). The Rise and Fall of the CIA. In *The Oxford Handbook of National Security Intelligence*. Oxford University Press, 122-137.

Kentish, B. (November 6, 2016). SAS in Iraq given `kill list` of 200 British jihadis to take out. *The Independent*. Retrieved from. http://www.independent.co.uk/news/world/middle-east/sas-special-forces-hit-list-iraq-syria-isis-terrorist-attacks-drones-a7400756.html Access: 24/11/19

Lahneman, W. J. (2010). The need for a new intelligence paradigm. *International Journal of Intelligence and Counterintelligence*, 23(2), 201-225.

Lederman, G. N. (2005). Restructuring the intelligence community. *Peter Berkowitz: The Future of American Intelligence (Stanford: Hoover Institution Press, 2005)*, 65-102.

Levine, M. (September 27, 2017). FBI has 1,000 open investigations into violent white supremacy, domestic terror: Agency chief. *ABC News*. Retrieved from. http://abcnews.go.com/US/fbi-1000-open-investigations-violent-white-supremacy-domestic/story?id=50127366 Access: 24/11/19

Libo-on, A. (February 9, 2016). The growth of social media v 3.0. *Search Engine Journal*. Retrieved from. https://www.searchenginejournal.com/growth-social-media-v-3-0-infographic/155115/ Access: 14/11/19

Lim, K. (2016). Big Data and Strategic Intelligence, *Intelligence and National Security*, 31(4), 619-635.

Lucas, E. (April 27, 2019). The Spycraft Revolution. *Foreign Policy*. Retrieved from. https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/ Access: 29/02/20

Madeira, V. (2003). 'No Wishful Thinking Allowed': Secret Service Committee and Intelligence Reform in Great Britain, 1919–23. *Intelligence and National Security*, 18(1), 1-20.

Marten, K. (2019). Russia's use of semi-state security forces: the case of the Wagner Group. *Post-Soviet Affairs*, 35(3), 181-204.

Matey, G. D. (2013). The Use of Intelligence in the Private Sector, *International Journal of Intelligence and Counterintelligence*, 26(2), 272-287.

Mattern, T., Felker, J., Borum, R., & Bamford, G. (2014). Operational levels of cyber intelligence. *International Journal of Intelligence and Counterintelligence*, 27(4), 702-719.

Mazurova, N. (2016). Russia's Response to Terrorism. History and Implications for US Policy. *American Security Project*, 1-11.

McLaughlin, J. & Dorman, Z. (December 30, 2019). 'Shattered': Inside the secret battle to save America's undercover spies in the digital age. *Yahoo News*. Retrieved from. https://news.yahoo.com/shattered-inside-the-secret-battle-to-save-americas-undercover-spies-in-the-digital-age-100029026.html?soc_src=community&soc_trk=tw Access: 29/02/20

McNeil, P. P. (2008). The Evolution of the US Intelligence Community—An Historical Overview. In *Intelligence and National Security: The Secret World of Spies: An Anthology*, Oxford University Press, 5-20.

Milli Istihbarat Teskilati. *Bilim ve Teknoloji Uzmani*. Retrieved from. http://www.mit.gov.tr/iksayfasi/biltekuz.html Access: 22/11/19

Milli Istihbarat Teskilati. *Kronoloji*. Retrieved from. http://www.mit.gov.tr/text_site/kronoloji.html Access: 22/11/19

Milmo, C. (July 29, 2013). MI6 and MI5 `refuse to use Lenovo computers` over claims Chinese company makes them vulnerable to hacking. *The Independent*. Retrieved from. http://www.independent.co.uk/news/uk/home-news/mi6-and-mi5-refuse-to-use-lenovo-computers-over-claims-chinese-company-makes-them-vulnerable-to-8737072.html Access: 22/11/19

Moore, J. (July 25, 2017). How ISIS remote-controls its European operatives to commit an attack: 'be quick'. *Newsweek*. Retrieved from. https://www.newsweek.com/be-quick-how-isis-remotely-directs-its-operatives-commit-attack-europe-641448 Access: 12/02/20

Nakashima, E. & Gillum, J. (September 13, 2017). U.S. moves to ban Kaspersky software in federal agencies amid concerns of Russian espionage. *The Washington Post*. Retrieved from. https://www.washingtonpost.com/world/national-security/us-to-ban-use-of-kaspersky-software-in-federal-agencies-amid-concerns-of-russian-espionage/2017/09/13/36b717d0-989e-11e7-82e4-

f1076f6d6152_story.html?tid=ss_tw-amp&utm_term=.d620250ef133 Access: 22/11/19

National Cyber Security Centre (June 9, 2017). *About the NCSC*. Retrieved from. https://www.ncsc.gov.uk/information/about-ncsc Access: 22/11/19

Nicander, L. D. (2011). Understanding intelligence community innovation in the post-9/11 world. *International Journal of Intelligence and Counterintelligence*, 24(3), 534-568.

O'Halpin, E. (2005). The Liddell diaries and British intelligence history. *Intelligence and National Security*, 20(4), 670-686.

Perlman, S. M. (2018). US intelligence and communist plots in postwar France. *Intelligence and National Security*, 33(3), 376-390.

Popper, N. (August 18, 2019). Terrorists Turn to Bitcoin for Funding, and They're Learning Fast. The New York Times. Retrieved from. https://www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html Access: 12/02/20

Regens, J. L. (2019). Augmenting human cognition to enhance strategic, operational, and tactical intelligence. *Intelligence and National Security*, 34(5), 673-687.

Renz, B. (2016). Russia and 'hybrid warfare'. *Contemporary Politics*, 22(3), 283-300.

Robarge, D. (2010). Leadership in an Intelligence Organization: The Directors of Central Intelligence and the CIA. In *The Oxford Handbook of National Security Intelligence*, Oxford University Press, 485-501.

Rovner, J. (2013). Intelligence in the Twitter Age, *International Journal of Intelligence and Counterintelligence*, 26(2), 260-271

Rovner, J., & Long, A. (2005). The perils of shallow theory: Intelligence reform and the 9/11 commission. *International Journal of Intelligence and Counterintelligence*, 18(4), 609-637.

Rudner, M. (2006). Using financial intelligence against the funding of terrorism. *International Journal of Intelligence and Counterintelligence*, 19(1), 32-58.

Sanger, D. E. (April 24, 2016). U.S. Cyberattacks Target ISIS in a New Line of Combat. *The New York Times*. Retrieved from.

https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html Access: 29/02/20

Secret Intelligence Service. *Science and Technology*. Retrieved from. https://www.sis.gov.uk/science-and-technology.html Access: 11/22/17

Singh, S. J. (2019). The U.S. Intelligence Enterprise and the Role of Privatizing Intelligence. *Belfer Center for Science and International Affairs*, Harvard Kennedy School.

SM Irwin, A. & Raymond Choo, K. K., & Lui, L. (2014). Money laundering and terrorism financing in virtual environments: A feasibility study. *Journal of Money Laundering Control*, 17(1), 50-75.

Smith, D. (2004). Dark side to US intelligence reform. *Washington Quarterly*. 14.

Stimson, C. & Habeck, M. (2016). Reforming Intelligence: A Proposal for Reorganizing the Intelligence Community and Improving Analysis. *The Heritage Foundation*.

Struyk, R. (August 15 ,2017). By the numbers: 7 charts that explain hate groups in the United States. *CNN*. Retrieved from. http://www.cnn.com/2017/08/14/politics/charts-explain-us-hate-groups/index.html Access: 24/11/19

Taylor, G. (October 1, 2015). CIA goes live with new cyber directorate, massive internal reorganization. *The Washington Times*. Retrieved from. https://www.washingtontimes.com/news/2015/oct/1/cia-goes-live-with-new-cyber-directorate-massive-i/ Access: 22/11/19

Tremblay, P. (November 6, 2016). Post-coup shake-up at Turkey's intelligence agency. *Al- Monitor*. Retrieved from. https://www.al-monitor.com/pulse/originals/2016/11/turkey-post-botched-coup-shake-up-at-turkish-intelligence.html Access: 22/11/19

Tu, K. V. and Meredith, M. W. (2015). Rethinking virtual currency regulation in the Bitcoin age. *Wash. L. Rev*., 90, 271-348.

Turpin, J. B. (2014). Bitcoin: the economic case for a global, virtual currency operating in an unexplored framework. *Indiana Journal of Global Legal Studies*, 21(1), 335-368.

Ünver, H. A. (July 2018). Digital Open Source Intelligence and International Security: A Primer. *Cyber Governance and Digital Democracy 2018/8*. EDAM, Istanbul.

Vovchenko, G. N. Tischenko, N. E., Epifanova, V. T., & Gontmacher, B. M. (2017). Electronic currency: The potential risks to national security and methods to minimize them. *European Research Studies Journal*, 20(1), 36-48.

Walsh, P. F. (2017). Making future leaders in the US intelligence community: challenges and opportunities, *Intelligence and National Security*, 32(4), 441-459.

Warner, M. (2012). Reflections on technology and intelligence systems. *Intelligence and National Security*, 27(1), 133-153.

Warner, M., & McDonald, J. K. (2005). *US intelligence community reform studies since 1947*. Central Intelligence Agency, Washington DC, Center for Study of Intelligence.

Wirtz, J. J. (2017). The Cyber Pearl Harbor, *Intelligence and National Security*, 32(6), 758-767.

Zegart, A. B. (2005). September 11 and the adaptation failure of US intelligence agencies. *International Security*, 29(4), 78-111.

Zegart, A. B. (2006). An empirical analysis of failed intelligence reforms before September 11. *Political Science Quarterly*, 121(1), 33-60.