Roman Kolodii[1]

THE IMPACT OF CYBER DOMAIN ON ESPIONAGE AS A METHOD OF INTELLIGENCE COLLECTION

Abstract

Traditional espionage has always been a vital tool allowing states to collect important information pertinent to their national security. The arrival of cyber, however, has created new opportunities and vulnerabilities for the process of intelligence gathering that have tangibly affected the efficiency of national intelligence agencies. This essay asks in what ways cyber domain changed conventional espionage and how profound this impact was for the activities of intelligence organizations across the world. The main argument of this research is that cyber has transformed the character of espionage by making it more comprehensive, cost-efficient and much less human-dependent, as well as far less attributable. But more importantly, cyber domain has also altered the nature of spying by narrowing substantially the gap between peacetime routine intelligence collection and cyberwarfare.

Key words: espionage, cyberespionage, cyber domain, cyberwarfare, HUMINT, SIGINT

Анотація

Традиційне шпигунство завжди було важливим інструментом, яке дозволяло державам добувати важливу інформацію для їхньої національної безпеки. Постання та розширення кіберпростору створило нові можливості та уразливості в процесі збору розвідувальних даних, які відчутно вплинули на ефективність національних спецслужб. Дана стаття має на меті з'ясувати, яким чином кіберпростір змінив традиційне шпигунство та наскільки глибоким був його вплив на діяльність розвідувальних організацій. Дане дослідження встановило, що кіберпростір змінив характер шпигунства, зробивши його більш комплексним, ресурсно-ощадним і набагато менш залежним від людини, а також істотно ускладнив процес присвоєння

[1] A second-year student of Master's Programme in International Relations at the Institute of International Relations, Taras Shevchenko National University of Kyiv

Supervisor: Dr. Yuriy Skorokhod, professor at the Chair of International Organizations and Diplomatic Service, Institute of International Relations, Taras Shevchenko National University of Kyiv

відповідальності. Однак найважливішим у цьому контексті є те, що кіберпростір трансформував природу шпигунства, розмивши кордон між звичайним збором розвідданих в мирний час та засобами й прийомами ведення військових дій у кіберпросторі.

Ключові слова: шпигунство, кібершпигунство, кіберпростір, кібервійна, HUMINT, SIGINT

Аннотация

Традиционный шпионаж всегда был важным инструментом, позволяющим государствам добывать важную информацию для их национальной безопасности. Однако возникновение и расширение киберпространства создало новые возможности и уязвимости в процессе сбора разведывательных данных, которые ощутимо повлияли на эффективность национальных спецслужб. Данное эссе имело целью выяснить, каким образом киберпространство изменило традиционный шпионаж и насколько глубоким было его влияние на деятельность разведывательных организаций. Данное исследование установило, что киберпространство изменило характер шпионажа, сделав его более комплексным, экономным и гораздо менее зависимым от человека, а также существенно осложнило процесс присвоения ответственности. Однако самым важным в этом контексте является то, что киберпространство трансформировало природу шпионажа, размыв границу между обычным сбором разведданных в мирное время и средствами и приемами ведения военных действий в киберпространстве.

Ключевые слова: шпионаж, кибершпионаж, киберпространство, кибервойна, HUMINT, SIGINT

INTRODUCTION

The high-grossing superhero film series X-Men launched at the turn of the century was almost a biblical revelation of what would materialize very shortly. In order to prevent the main villain–Magneto–from bringing his malign intents to fruition, the leader of protagonists Professor Xavier, endowed with extraordinary telepathic powers, used special equipment that enhanced his abilities tremendously – Cerebro. This mechanism allowed him to find any mutant in the world and specify their appearance, location, and even behavior. Cerebro was an important device that helped Professor Xavier and his team to recruit mutants in order to eventually disrupt evil plans of Magneto.

Although initially perceived as an imagined invention possible only inside the Marvel universe, Cerebro is now part of our everyday reality. Nowadays, intelligence agencies and non-state companies have the capacity to connect to virtually every individual and extract relevant data about his identity or behavior using cyber capabilities at hand. The great migration of humankind into cyberspace coupled with digitization of critical infrastructure formed a Cerebro-like environment which remains within the reach of state-sponsored intrusions in the form of cyberespionage.

Throughout the centuries, traditional spying has long allowed states to collect foreign information pertinent to their national security. The arrival of cyber, however, has created new opportunities and vulnerabilities for the process of intelligence gathering that have tangibly affected the efficiency of national intelligence organizations. On one hand, the knowledge of its implications is important for the policies and routines of intelligence agencies. On the other hand, it also crucial for the understanding of how individuals and non-state actors in general are being exploited and what risks are attached to their daily activities within cyberspace.

The essay, therefore, addresses a burning issue of cyberespionage in an increasingly interconnected world of governments, companies and people. The main avenue of this research is espionage as a prominent method for intelligence collection. More specifically, the essay asks in what ways cyber domain changed conventional espionage and how profound this impact was for the activities of intelligence agencies across the world. The main argument of this research is that cyber has transformed the character of espionage and also its nature by narrowing substantially the gap between peacetime routine intelligence collection and cyberwarfare.

As for the semantics of this research, by traditional espionage we imply ‘the non-consensual collection of confidential information that is under the control of another actor’ (Buchan, 2019, p.2) through the means of

human and signal intelligence (and its subcategories such as COMINT and IMINT). For the sake of this essay, human intelligence will refer to the activities of intelligence agents in the physical realm, whereas signal intelligence will mean the use of high frequency antennas, satellites, stealthy jets, and drones 'to capture electronic transmissions emanating from the territory of other states and […] observe and monitor events on Earth' (Buchan, 2019, p.3). By cyberespionage we mean 'deliberate activities to penetrate computer systems or networks used by an adversary for obtaining information resident on or transiting through these systems or networks' (Banks, 2017, p.513). In this essay we will discuss both political and economic cyberespionage, as well as extraterritorial surveillance as a subcategory of cyber spying (Jupillat, 2017, p.953). Although we agree with an opinion that cyberespionage should be viewed as part of espionage efforts in general (Duvenage and von Solms, 2013, p.1), we do underscore that both contrast in many ways, as cyber enables some unique features of intelligence collection which traditional spying fails to ensure.

Since the existence or possibility of cyberwar is highly contested, in this essay we will refer to the notion of cyberwarfare, rather than cyberwar. By the former we mean techniques, methods, weaponry and strategies designed to defeat an adversary within cyberspace. This notion will give us some flexibility, as an occasional use of cyberwarfare does take place in modern world, though it hardly qualifies for an all-out cyberwar between nations. Throughout this essay we will compare peacetime conventional espionage to peacetime cyberespionage, although the latter would be questioned eventually. We will not discuss ethical dimension of espionage, nor will we engage with domestic law on spying. Instead, we will focus mostly on allegedly state-sponsored conventional and cyber espionage and its (non-)regulation within international law.

The discussion of the topic will unfold as follows. In the next three chapters we will identify and closely scrutinize three most salient features of cyberespionage that make it different from its conventional analogue. Not only we will explain how these characteristics shape the overall process of intelligence collection (as opposed to other sections of intelligence cycle), but we will also present counterarguments to our points that exist within scholarship and carefully dismantle them. In the end we will arrive at the conclusion that cyber domain has transformed espionage profoundly, altering not only the character, but also the nature of espionage, making it less human-dependent and more warfare-related.

CYBERESPIONAGE V CONVENTIONAL ESPIONAGE: THREE PERSPECTIVES

Due to cyber, espionage has become less human-related and more computerized, lowering dramatically the risks for human agents and costs of data extraction

Cyber has tangibly transformed the ways and means which are deployed for the purpose of intelligence collection. Previously, governments had long focused on dispatching their staff directly to particular destination to conduct covert operations. Working highly clandestinely, foreign agents normally infiltrated government bodies, military units, or other specific organizations that possessed sought-after information. Their chores mostly included obtaining precise data on military, financial or political situation in the targeted country, penetrating facilities with restricted access, copying or stealing objects that retained valuable information, or inserting spying sensors or other technical equipment. In addition, spies were also involved in surveillance of certain individuals suspected of possessing important knowledge or recruiting them for a long-term collaboration. Over time this type of espionage supported largely by the means of human intelligence has been complemented with cutting-edge technologies like stealthy jets, satellites or, most recently, drones. These vehicles facilitated intelligence collection, as they helped to conduct reconnaissance of military objects located on a foreign territory, intercept and decipher signal communications or track individuals thus establishing links between them and suspicious groups, and all of these have been achieved in a much more effective, comprehensive and large-scale manner. In this regard, espionage based on human intelligence and SIGINT was in all instances characterized by a pronounced importance of humans who acted either as spies or operators of spying devices.

Cyber has reduced the significance of human factor in the process of intelligence gathering dramatically. In contrast to traditional espionage where humans played an instrumental role by physically approaching and penetrating sources of valuable data, cyberespionage saw the replacement of human agents with computer programs. A malware used to exercise an attack against foreign communications network normally does all the job of traditional spies. After having being launched, the program travels the whole communication chain down to a targeted computer system, penetrates inner logs, and then accesses embedded databases and exfiltrates confidential and classified documents. What traditionally has necessitated physical engagement of highly-trained individuals now is achievable through the use

of computer worms. To illustrate, spear phishing attacks designed to acquire large amounts of valuable information on the United States' Patriot missile system, UK F-35 program, and the networks of Mitsubishi Heavy Industries (Matsubara, 2014, p.89) consisted just in sending e-mails containing 'PDFs or other attachments, or a hyperlink that installs a remote-access tool when opened.' (Segal, 2013, p.40) This tool allowed foreign intruders to get access to classified information of those organizations without the reliance on human agents.

The tremendous operational potential of computer worms can be further exemplified by other cases of cyberespionage activities. For instance, GhostNet's Trojan, disseminated in 2007, not only copied the needed files from infected computers, but also was capable of controlling the systems in real time, even switching on devices such as web cameras or embedded microphones (Adkins, 2013, p.5). Red October attack, in its turn, was one of the first to allow for penetrating not only computers but 'also smart phones and networking hardware such as Cisco switches and routers' (Adkins, 2013, p.5), increasing the scope of intelligence collection substantially. Cyberespionage, in this respect, lent itself well to uncovering and exploiting vulnerabilities of human-to-machine interactions, which are now pervasive, whereas conventional HUMINT was by and large confined to human-to-human communication.

Computer programs also have the capacity to collect immense torrents of variegated data that by far surpasses abilities of humans. Cyber, in this respect, allows intelligence agencies to collect meta-data through data-mining (gathering information about an individual from various devices and sources to create digital dossier) and dataveillance (monitoring electronic footprint of individuals as they interact with computers by logging in websites) (Bellaby, 2016, p.301). The amounts of bulk data collected through the use of malware are so diverse and multifaceted that it even makes possible to build predictive models of human behavior and gauge the possibility for future attacks (Bellaby, 2016, p.301). This allows 'for unprecedented mass-scale data-gathering opportunities' that modified the nature of espionage in its Hegelian idea of quantity becoming quality (Jupillat, 2017, p.976). This was not possible by means of conventional espionage that mostly relied on sporadic and dispersed pieces of information.

As compared to traditional SIGINT, cyberespionage has also proved to be diminishingly human-dependent. Many devices that enable surveillance are still handled manually by human operators. Even unmanned aerial vehicles that boast reputation of being increasingly autonomous still require at least a remote presence of human operator. In contrast to this, malware used to hijack foreign computers and steal data acts more autonomously than drones, for instance. These programs' code allows them

to penetrate and spread within communication networks, as well as detect sought-after information and manipulate it without manual control of humans. For instance, the breach of U.S. Defense Department's global secure intranet called SIPRNET was possible due to a spyware inserted through a flash drive that was capable of replicating itself automatically (Rid, 2013, p.21). However, manual control of such malware is still used widely to achieve greater delicacy in the execution of the attack. That being said, many recent studies on the application of deep learning techniques to the upgrading of spying malware suggest that in future these programs will be increasingly autonomous (Jupillat, 2017, p.976).

In addition to a far more nuanced penetration into confidential systems, impressive data-gathering scale and increasingly autonomous operation, cyberespionage has also dramatically reduced the human-side risks of intelligence collection. Unlike traditional espionage, when 'the risk taken by the agent could be self-deterring' (Jupillat, 2017, p.975), cyberespionage that allows governments to act without human agents and remotely through computer programs reduces risks to human life dramatically. Furthermore, many states now recruit private actors – companies or individuals – to conduct exploitation of foreign communications networks which are known as 'partial state actors' or […] 'privateers' (Nigel, 2015, p.67). The involvement of non-state actors in the process of intelligence collection through cyberespionage made state intelligence agencies more discreet in that they can keep their hands 'clean', their reputation intact and their agents safe while still obtaining relevant information from abroad.

Therefore, cyber has drastically reduced the instrumental role of humans in the course of espionage efforts serving as evidence that cyber domain has transformed the espionage practices. It made intelligence collection less human-dependent, more autonomous and computerized, exceedingly comprehensive, low risk and, importantly, cost-efficient when compared to resource-consuming HUMINT operations or expensive SIGINT projects.

Cyber has made intelligence collection ex-territorial and de-personified thus rendering attribution of espionage extremely difficult if possible

Governments have been constantly engaged in espionage on a foreign territory to obtain information critical to their national security. As each nation considers intelligence as a vital tool to anticipate hostile activity of other states, espionage has become a common practice favored by all states. Some of them limit the scope of intelligence gathering to special units of

embassies located abroad. Others complement these capabilities with secret agents dispatched there from a spying country or recruited on the ground from local community. Although spying in its own right serves as an indication of distrust among nations both symbolically and empirically, it increases predictability and fosters stability (Libicki, 2018, p.111), as governments can reassure themselves about risks to their national security from abroad and undertake proper preparatory measures. Conventional espionage, therefore, has been mutually tolerated and thus customary to international communication.

However, the underlying reason why trust could be achieved through reciprocal spying was that governments could attribute these activities to particular countries and analyze the rationale behind these controversial efforts. Mutual reassurance in case of tolerated espionage was therefore nurtured by the understanding of who was involved and for what purpose. Although gaining this knowledge normally required laborious measures and extra resources, it nonetheless used to be rather credible. To illustrate, in case of HUMINT, such measures as counterintelligence, deception, detention, interrogation and observation allowed targeted country to establish identities of perpetrators and their nationalities, as well as other relevant information about the purpose and specifics of their mission. In case of surveillance and reconnaissance activities, governments could attribute spying devices by detecting them and identifying their technical characteristics. Since countries conduct information sharing on their military capabilities, although to a limited extent, the technical characteristics of surveillance vehicles could suggest that they were operated by the government of the country A that manufactures vehicles with similar distinctive design, rather than the country B. Attribution of conventional espionage, therefore, has been achievable with rather high a degree of credibility.

Cyber has made the problem of attribution of espionage exceedingly intricate if resolvable. The nature of cyber domain allows governments to hide the most information about cyberattack extremely effectively. Most cyberespionage activities are carried out anonymously due to highly resistant encryption techniques used by hackers. These techniques become ever more ubiquitous as they were used, for instance, by ISIS with its encryption chat systems that prevented CIA surveillance (Banks, 2017, p.517). Al-Qaeda, too, uses PGP to encrypt messages or PGPfone to shield voice communications (Adkins, 2013, p.4). Cyberespionage attack called Operation Aurora launched in 2009 and targeting zero-day exploits of Adobe reader ‘used several levels of obfuscation including encryption, up to three times, to hide itself from normal detection’ (Zetter, 2010). The encryption methods that are more sophisticated and simultaneously more available

oftentimes make the task of establishing the identity of hackers impossible, as, in contrast to traditional espionage, their physical features and digital traces are concealed. It is also extremely difficult to establish their nationality, as they conduct their activities remotely and cannot be reached and interrogated. Attribution thus becomes 'a serious technical problem [that] makes controlling cyber exploitation more difficult than keeping tabs on traditional spying' (Banks, 2017, p.519).

Surprisingly, even location of the attackers often speaks little about which foreign government should be accused of espionage. Cyber capabilities allow for hijacking computers in the targeted country and launching attacks from there, or from a third country, thus causing much confusion about who stands behind espionage – local actors or nationals of another country that rely on proxies, or actors from an unrelated jurisdiction (Edwards et al, 2017, p.2825). Unlike SIGINT that allows agencies to establish the source of a signal, cyberespionage rejects the possibility of credibly tracing the source of a cyberattack. This makes governments even more suspicious about their counterparts, aggravates general confusion and erodes trust. Although credibility of these allegations falters, governments do attribute cyberespionage to each other. Companies, like Google in 2009, report the countries where cyberattacks ostensibly were originated, and intelligence agencies sometimes establish the names of hackers behind them. The principle that allows governments to conduct attribution is as follows – if the source of attack 'is located on a certain territory then the data is considered to belong to that territory' (Sarbu, 2017, p.128). However, it is rarely backed up by reliable evidence, as 'online identities can be hidden, packet flows redirected and vulnerable machines used as proxies' (Wangen, 2015, p.186), which makes ascribing blame lacking sufficient material support.

Therefore, unlike conventional spying, cyber has made the problem of attribution of espionage barely addressable due to ex-territorial and de-personified character of the activity when conducted within cyberspace. In most instances attribution is shaped by current political agenda that reflects geopolitical struggle rather than being an outcome of forceful post-attack forensics.

Cyber has blurred the lines between espionage as a peacetime intelligence routine and as a part of cyberwarfare

In contrast to wartime espionage, governments accorded little attention to the regulation of peacetime spying, and left abundant normative loopholes

generously exploited by foreign entities. In fact, governments made reciprocal espionage a valuable tool to obtain information about each other and by so doing reduce uncertainty about intentions of their counterparts. The absence of international regulation of peacetime spying allowed countries to violate the sovereignty of each other occasionally without severe repercussions in the form of courting accusations of using force or launching a blatant aggression. If spies are apprehended on a foreign territory, they would normally be persecuted and extradited, expelled or exchanged via diplomatic channels (Banks, 2017, p.523). In some cases they might be charged with a criminal offence and incarcerated. If countries detect foreign aerial vehicles conducting SIGINT over their territory, they might intercept it with national jets and oust it, or, in the worst case scenario, down it with air defense missiles. In such cases this might lead to diplomatic standoff or political escalation, but rarely to any sort of war activity between the opponents. Instead, normally both human intelligence-based espionage, and surveillance conducted by aerial vehicles have been deemed an acceptable practice among nations.

Cyber has made the fault line between espionage as an intelligence activity and as a warfare effort much less distinguishable. Some scholars claim that cyberespionage cannot pass the threshold to be deemed an instance of cyberwar since it usually does not upset the work of digital and critical infrastructure and thus does not have destructive purpose. However, although some discern cyberespionage from a cyberattack *par excellence*, (Libicki, 2018, p.111) most experts consider cyber spying technically as a cyberattack, as its effects might be disruptive for the functioning of electronic systems in several ways.

Firstly, cyberattacks aimed just at accessing and exfiltrating data are often not distinguishable from those designed to inflict harm or halt the work of communication networks, especially during the stage of malware deployment. ‘A malware implant designed for cyberespionage is often identical to one designed for cyberattack, discovering and attributing one in a critical system could easily be viewed as a direct precursor to attack.’ (Libicki, 2018, p.111) Some organizations like NATO, however, make clear distinction between computer network exploitation (CNE), which is what we normally call cyberespionage, and computer network attack (CNA) that inflicts tangible damage (Sarbu, 2017, p.131). However, in practice it is extremely difficult to identify the nature of intrusion based on this distinction. The hacking of American company Telvent, for instance, raised doubts as to whether foreign perpetrators just tried to copy sensitive industrial data or planned ‘to plant malware that would eventually shut down the energy system’ operated by Telvent (Segal, 2013, p.42).This creates a constant risk

that cyberespionage can evolve into destructive assault on computer systems any time.

Secondly, spying malware often contains so-called dual-payload, which means that along with collecting and sending back local data, it is also equipped with a capability to launch an attack against the boot sequence of machines thus suspending their work and causing material damage. 'The payload's first role is merely data observation and collection, activity that falls under the espionage category. The second role is to neutralize the system upon command. Whether the deployment of such a payload amounts to espionage or rises to the level of the threat or use of force is a difficult question to resolve' (Pelikan, 2012, p.366).

Thirdly, cyberespionage attacks can be used to test and probe cybersecurity of communication networks to find vulnerabilities and weaknesses that foreign governments can further exploit while conducting an offensive cyberattack for destructive purposes. In 2009 Google stated that an espionage attack launched against it, along with theft of proprietary information, gathered 'insights about security weaknesses' of Google's network system (Segal, 2013, p.43). This has raised concerns about espionage being a disguise for reconnaissance to prepare the battlefield, as it leaves behind 'software programs that could be used in the future to disrupt […] critical infrastructure.' (Hjortdal, 2011, p.6) Hence frequent cyber intrusions for the purpose of espionage cumulatively weaken the systems and might cause visible collateral damage.

Finally, some types of cyberespionage, such as economic espionage, when hackers steal volatile commercial data, can upset the work of companies or financial markets that are highly susceptible and dependent on trust and confidentiality (Banks, 2017). In this case cyberespionage leads to frustrated financial situation on the market and immense material losses for companies and governments. This economic damage effectively overcomes the argument that cyberespionage falls short of meeting the threshold of use of force because 'there is no physical damage or loss of life.' (Banks, 2017, p.523) In fact, material damage caused by cyberespionage and foreign surveillance is indeed considerable, as it incurs enormous costs of $300-600 billion annually (Banks, 2017, p.521). Other estimates show that in 2008, for instance, 'in the aggregate, companies across the globe lost more than $1 trillion from security breaches' (O'Hara, 2010). This means that despite the absence of damage to physical infrastructure, cyberespionage adversely affects economic infrastructure of states thus going far beyond the routine practice of intelligence collection.

The technical and economic considerations provided above prove that, unlike traditional espionage and surveillance, cyberespionage can bring severe damage that exceeds the scope of routine peacetime intelligence

collection activities. Apart from these, there are also legal and military aspects of cyberespionage that make it destructive thus qualifying it as part of cyberwarfare. From legal point of view, cyberespionage might present some form of intervention. For instance, the theft of sensitive information about more than 20 million American government employees in 2014, although was orchestrated remotely, violated the territorial sovereignty of the US by breaching servers located on US soil. Some argue that cyberespionage, in this and other instances, is not an act of coercion of other country's 'choice of a political, economic, social and cultural system, and the formulation of foreign policy,' which is otherwise needed to qualify cyberespionage as intervention under ICJ's 1986 Nicaragua judgement (Terry, 2018, p.620). However, the fact that a targeted country is robbed of sensitive information means that it was deprived of 'the opportunity to make a sovereign decision on who it wanted to share information […] with', which meets the threshold of coercion and therefore illegal intervention under international law (Terry, 2018, p.621).

On the military side of the equation, cyberespionage serves as a means of deterrence or reconnaissance which qualifies it as part of cyberwarfare, but not necessarily cyberwar itself. Some noisy cyberattacks allegedly launched by foreign governments to obtain data from U.S. critical infrastructure facilities, for instance during Titan Rain attack in 2006, were regarded as a warning that 'the US homeland may not be immune to attack' in the event of a real-world conflict (Segal, 2013, p.44). Apart from that, according to recent studies, cyberespionage adversely affects military industry as it allows countries to steal military know-how and reverse engineer it, thus giving a competitive edge for foreign military strategies (Gilli, 2018). All of this makes cyberespionage both a military deterrent that pre-empts foreign cyberattacks (Iasiello, 2016) and a 'cyberwarfare capability' (Hjortdal, 2011) thus locating it within a cyberwarfare, rather than peacetime cyber intelligence, context. 'As a matter of fact, cyberespionage marked the beginning of what is now commonly referred to as cyberwarfare, and continues to be its most common manifestation today, consistently ahead of cyber sabotage among state-sponsored operations.' (Jupillat, 2017, p.934)

However, cyberespionage on its own does not mean the state of cyberwar, as it is 'below-the-threshold' of the armed attack (Lubin, 2018). Apart from that, cyberespionage, although offensive in nature, does not meet a Clausewitzian criteria of being 'most importantly – politically attributed' (Rid, 2013) and therefore cannot amount to an act of cyberwar. However, overall, cyberespionage, although conceived and conducted primarily as a peacetime intelligence collection practice, is becoming increasingly part and

parcel of cyberwarfare, thus contrasting sharply with peacetime conventional spying.

CONCLUSION

Cyber domain has significantly transformed the character and nature of espionage as a method of intelligence collection. Due to the introduction of spying malware that can collect immense amounts of diverse data and replicate autonomously, espionage became more comprehensive, cost-efficient and much less human-dependent, as the main instrumental function, in contrast to conventional spying, rests with computer programs. This has reduced human-side risks dramatically. Secondly, cyber has made espionage ex-territorial and largely de-personified, as it is extremely difficult and yet rarely possible to credibly attribute espionage activities to foreign entities within cyberspace. Finally, unlike conventional peacetime spying, cyberespionage cannot be considered solely as a routinized intelligence collection practice, as it exhibits characteristics of cyberwarfare in several ways:

- cyberespionage is often indistinguishable from destructive cyberattacks which raises risks for governments and other targeted organizations;
- spying malware often contain dual payload which can be enable data exfiltration and also derailment or destruction of inner electronic systems;
- cyberespionage in economic and military spheres causes severe material damage and losses for governments, companies and more generally financial markets;
- cyberespionage involves intrusion into foreign servers thus qualifying as a coercive activity and even intervention into internal affairs. From a military point of view, cyberespionage spots vulnerabilities of targeted systems and subsequently weakens them, thus allowing foreign entities to prepare ground for more destructive cyberattacks.

Overall, unlike conventional spying, this makes cyberespionage inherently a destructive activity that makes it a cyberwarfare capability, rather than only a peacetime intelligence collection technique. The evidence provided allows us to conclude that cyber domain has changed the character and nature of espionage to a profound extent.

BIBLIOGRAPHY

1. Buchan, Russell 2019, "Introduction." Cyberespionage and International Law. Oxford: Hart Publishing,. 1–12. Bloomsbury Collections
2. Banks, W.C. 2017, "Cyberespionage and electronic surveillance: beyond the media coverage", Emory Law Journal, vol. 66, no. 3, pp.513
3. Jupillat, N. 2017, "From the Cuckoo's Egg to Global Surveillance: Cyberespionage that Becomes Prohibited Intervention", North Carolina Journal of International Law, vol. 42, no. 4, pp. 934.
4. Duvenage, P. & von Solms, S. 2013, "The case for cyber counterintelligence", IEEE, pp. 1.
5. Matsubara, M. 2014, "Countering Cyber-Espionage and Sabotage: The Next Steps For Japanese-Uk Cyber-Security Co-Operation", RUSI Journal, vol. 159, no. 1, pp. 86-93.
6. Segal, A. 2013, "The code not taken: China, the United States, and the future of cyberespionage", Bulletin of the Atomic Scientists, vol. 69, no. 5, pp. 38-45.
7. Adkins, G. 2013, "Red Teaming the Red Team: Utilizing Cyberespionage to Combat Terrorism", Journal of Strategic Security, vol. 6, no. 3, pp. 1-9.
8. Bellaby, R.W. 2016, "Justifying Cyber-intelligence?", Journal of Military Ethics, vol. 15, no. 4, pp. 299-319.
9. Rid, T. 2013, “Cyberwar will not take place”, Hurst & Company, London.
10. Nigel Inkster 2015, “Cyberespionage”, Adelphi Series, 55:456, 51-82,
11. Libicki, M.C. 2018, "Drawing inferences from cyberespionage", NATO CCD COE, pp. 109.
12. Kim Zetter, “Google Hackers Targeted Source Code of More Than 30 Companies,” Wired Magazine, January 13, 2010, available at: http://www.wired.com/threatlevel/2010/01/google-hack-attack/.
13. Edwards, B., Furnas, A., Forrest, S. & Axelrod, R. 2017, "Strategic aspects of cyberattack, attribution, and blame", Proceedings of the National Academy of Sciences of the United States of America, vol. 114, no. 11, pp. 2825-2830.
14. Sarbu, S. 2017, "The cyber threat and the problem of information security. A critical analysis of the concepts of cyber-

power and cyber-space", Annals – Series on Military Sciences, vol. 9, no. 1, pp. 126-138.

15. Wangen, G. 2015, "The Role of Malware in Reported Cyberespionage: A Review of the Impact and Mechanism", Information, vol. 6, no. 2, pp. 183-211.

16. Pelican, L. 2012, "Peacetime cyber-espionage: a dangerous but necessary game", CommLaw Conspectus, vol. 20, no. 2, pp. 363.

17. Hjortdal, M. 2011, "China's Use of Cyberwarfare: Espionage Meets Strategic Deterrence", Journal of Strategic Security, vol. 4, no. 2, pp. 1-24.

18. O'Hara, G. 2010, "Cyber-espionage: a growing threat to the American economy", CommLaw Conspectus, vol. 19, no. 1, pp. 241.

19. Terry, P.C.R. 2018, "“Don't Do as I Do”—The US Response to Russian and Chinese Cyberespionage and Public International Law", German Law Journal, vol. 19, no. 3, pp. 613-626.

20. Gilli, A. & Gilli, M. 2019, "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyberespionage", International Security, vol. 43, no. 3, pp. 141-189.

21. Iasiello, E. 2016, "China's Three Warfares Strategy Mitigates Fallout from Cyberespionage Activities", Journal of Strategic Security, vol. 9, no. 2, pp. 45-69.

22. Lubin, A. 2018, "Cyber law and espionage law as communicating vessels", NATO CCD COE, pp. 203.