Hybrid nature of modern threats for cybersecurity and information security

Oleksandr TSARUK
CSc, MBA, Ecole Des Ponts Business School, Champs-Sur-Marne, France
E-mail address: o.tsaruk@pontsbschool.com

Maria KORNIIETS
MA, Institute of International Relations, Taras Shevchenko Universiy of Kyiv, Kyiv, Ukraine
E-mail address: mariakorniiets@gmail.com

Abstract
The paper deals with phenomena arising from radical disruptions in numerous spheres of human activity that challenge the conventional understanding of security. Authors endeavour to contribute to understanding of these changes and the emerging paradigm. The notions of cyber security, information security in relation to the cyber-physical systems security, and information security in broader sense which describes safeguarding the information flows to cyberspace and media were considered. Authors explore modern manifestations of these threats, and then dive into the hybrid nature of the threats to cyber- and information security, describing cyber threats and cyber attacks as merged with existing 'conventional' techniques. The examination of hybrids threats - the cyber leverages to diplomacy, the practice of cyber retaliation, cyber sabotage and espionage, cyber weapons and the cyber arms race - was given.

Keywords: hybrid threats, cyber security threat, information security threat, categorization of threats.

1.Introduction
The changes associated with rise of information and communication technology (ITC) are ubiquitous. Some suggest that we are facing the 'Fourth Industrial Revolution' [1], others speak of the 'Third Wave of the Internet' [2], or argue that we're now part of the 'information' and 'knowledge' society [3]. These developments need to be properly analysed and put into a perspective, since alongside benefits come challenges and escalating threats of cyber domain.

The views on cybersecurity face transformations themselves, as the type of damage done in cyberspace changes. The attacks have become more devastating, evolving from spying and DDoS attacks in the early days to doing severe physical damage to the infrastructure and influencing public opinion on critical domestic affairs and interfering in elections.

In order to explore the changes in international relations, we set four tasks. First, we argue that 'US-NATO-European Union' and 'Chinese-Russian Approach' do not contradict each other, and can be combined into the common notion of 'cybersecurity' and 'information security'. The combination of these notions reflects the changing nature of the threats in cyberspace. Second, we look into the treats to cyber and information security of last five years and latest related trends. Third, after literature review hasn't shown cyber threat classifications applicable for international relations that can be extended to include information security, we proposed a categorisation of threats to cyber and information security. Lastly, we describe the phenomena emerging on the intersection of international politics and communication technology: cyber leverages to diplomacy, retaliation for cyber attacks, cyber sabotage and espionage, propaganda, cyber troops, weapons and arm race.

2. Two approaches to cyber and information security

There are two basic approaches to understanding 'cybersecurity' and 'information security' according to Aapo Cederberg [4] . The first one is US/ NATO/ EU vision of information security as a part of cybersecurity. The second one is a so-called 'Chinese-Russian Approach', that sees cybersecurity as a part of information security.

One of the latest definitions of the cybersecurity notions was given by Canadian government in the document considered by NATO Cooperative Cyber Defence Centre of Excellence [5] as Cyber Security Strategy of Canada: '*Cybersecurity is the protection of digital information and the infrastructure on which it resides. Cybersecurity addresses the challenges and threats of cyberspace in order to secure the benefits and opportunities of digital life.*' [6].

National Cyber Security Agenda of Denmark defines cybersecurity as 'the entirety of measures to prevent damage caused by disruption, failure or misuse of ICT and to recover should damage occur' [7]. At the same time, 3rd National Cyber Security Strategy of Luxembourg [8] refers to Recommendation ITU-T X.1205 where cybersecurity was showed as a more complex phenomenon - a 'collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies can be used to protect the cyber environment, its organization and its user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment...' [9].

The national law on the basic principles of ensuring cyber security of Ukraine [10] which defined the cybersecurity as 'safety of the *vital interests of human and citizen, society* and state when using cyberspace in case of which *sustainable development of information society* and the digital communication environment, timely identification, prevention and neutralization of real and potential hazards of national security of Ukraine in cyberspace are safeguarded'.

The Ukrainian definition goes beyond scope of two above mentioned as it has a much wider scope and deals not only with ICT and cyber-physical systems. Ukrainian definition touches human and society safety, and even concept of sustainability of information society.

The information security concept was developed to explain a different set of phenomena than cybersecurity. The 'Doctrine of Information Security of the Russian Federation' [11] defined the information security of the Russian Federation. The very same definition made it to the new doctrine of 2016 [12], as *'the state of protection of the individual, society and the State against internal and external information threats, allowing to ensure the constitutional human and civil rights and freedoms, the decent quality and standard of living for citizens, the sovereignty, the territorial integrity and sustainable socio-economic development of the Russian Federation, as well as defence and security of the State*.'

As we see, it deals with 'information threats' to public institutes and socio-economic development. The key difference is that human and society are claimed to be protected, and the weapon is the information which of course can be delivered thought cyber infrastructure, but analogue ways can also be used, such as conventional media, books and even public speaking events. Thus, this definition is not particularly specific, and allows to describe, for example, acts believed to be a hostile propaganda as a threat to information security that puts society in danger.

For most of western liberal societies, implementation of the information security strategies or even doctrines is a very uncommon case, as the realisation of basic human right in most cases contradicts with 'managing' information flows into social consciousness. Ukraine was also an example of such a liberal approach. The latest developments such as weaponised threats to national security made by external penetration into the national 'information sphere', raised the need to reinforce parity and to use innovative tools for further protection of national information space, while still facing a challenge of adhering to global ideals of the free flow of information.

Two years after the serious political crisis which causes 'Euromaidan' movement and hybrid active influence from Russia the "The Doctrine of Information Security of Ukraine" [13] was enforced with the primary aim of resisting propaganda and hybrid warfare in Ukraine.

Information Security Doctrine of Ukraine is focused on the currents treats, and the main goal of it was setting ground rules of national information policy to resist the weaponized information impact from Russian Federation in a state of hybrid war. It is very important that this document underlines that Ukraine is facing active hybrid war.

The document does not give the definition of the 'information security' directly, and it delineates it as a part of the state priorities in information space on ensuring *information security*:

- creation of an integrated system of informational threats evaluation;
- increasing regulatory efficiency of state authorities engaged in information space governance;
- legal mechanism searching, estimating, blocking and deleting from information space of state (not only Internet), and from Ukrainian segment of the Internet, for instance, information which causes threat for life and health of citizens, propagate war, ethnic and religious weaponization, nazi and communist ideology, calls for failing sovereignty etc.;
- need of cooperation with civil society to combat information aggression, disinformation and propaganda;
- safeguarding international image and reputation of Ukraine.

So, the concept of 'information security' is defined as the synthesis of measures which address questions of governance of information flows into social consciousness by Internet, media, and press. Therefore it can touch critical telecommunication infrastructure only as

the method of transmitting weaponized content of delivering the state governance but is not the subject of it directly as we have in case critical infrastructure for cybersecurity.

Ukraine also has implemented Cyber Security Strategy [14] with the aim of securing cyberspace, to the benefit of citizens, private sector and society in general. And, the goal of it is to safeguard transparency, availability, steadiness and safekeeping of cyberspace in Ukraine.

The outlook of the notion of 'information security' and 'cybersecurity' allows us to suggest that in countries facing hybrid treats trend to use the approach for the information security which define **information security** ***as system on state governed actions of the information flows into social consciousness with for safeguarding nation (citizens and residents) from weaponized influence from internal and external threats in form of propaganda, disinformation, violent ideologies, aggressive and disruptive social phenomena.***

Summarizing, we can say that difference in US/NATO/EU vision and 'Chinese-Russian Approach' comes from different definition of information security. The first is more specific and deals with information as an asset, without reference to any psychological influence it can have. The second one is broader, and, although it gives excessive power to a state, incorporates hybrid threats like propaganda, weaponized narrative, fake news and expectation management.

Furthermore, hereinafter in out article when referring to 'information security' we mean the security in a wider sense, namely the notion incorporating threat of public opinion manipulation and misinformation.

3. Modern threats for cybersecurity and information security

Before examining the hybrid nature of modern threats we need to analyse the latest developments and trends in the sphere. Moreover, in extension of our argument stating that the views do not contradict but can be complimentary, we examine the cases of threats to cyber and information security and offer a united categorization of the threats.

Scope of analysed cases

The misuse of a telegraph network in 19-century France is sometimes referred to as the first cyber attack in history [15] . As for the Internet networks, the Morris worm is one of the first infamous incidents of its kind, dating back to as early as 1988.

However, for the purpose of this article we will refer to cyber attacks starting from years 2006-2007. April 2007 marked the incident in Estonia, leading to the 'cyberwar' concept becoming mainstream [16]. Although it was not the first known cyber attack targeting a foreign government - the earlier examples including April 2001 US-China incident [17] and Titan Rain, a cyber espionage effort attributed to China, active at least since 2003 [18] - we believe it was among the first incidents that spurred a wider interest to the topic.

Since 2006-2007, more and more stories made it to media each year: cyberattacks during war in Georgia and a 'foreign spy' attack on US military websites in 2008, attack on South

Korean government websites, allegedly by Northern Korea, in 2009, and 2010 'Stuxnet' malware destroying centrifuges in Iran, etc. Thus, it makes a good starting point for our enquiry.

We pay more attention to the threats arising in the past 5 years, and the related trends. These developments we refer to as 'modern'.

Limitations

It should be noted that the ability to assess the current state of 'cyber weaponry' and the way they are being used by states or against them can be limited to the analysis of disclosed incidents. Since the matter is closely intertwined with national security and intelligence, the data is often classified, making it hard to see the undistorted picture. The number of the incidents, same as their original purpose and the malware creator, are largely up to speculation.

With this limitation in mind, we examined not only academic or government sources, but also related news coverages and reports by major antivirus providers.

Latest developments in cyber and information threats

To present the landscape of most recent changes in cyber and information security, we first list most notable cyber attacks of last five years (2013-2018) that are connected to politics; second, make a short overview of trends in the following areas: Connectivity/ Internet and Technology; Geopolitical landscape.

These spheres were chosen because we believe they are key to predicting future trends in cyber security: connectivity can show what kind of devices are likely to be affected due to increase exposure to Internet, technology - what kind of (new) devices are likely to be connected, and thus compromised. Geopolitical tendencies can shed light at the motivations behind future attacks.

List of modern attacks (2013-2018)

The last five years saw numerous cyber attacks (see Table 1). The year 2013 included Snowden disclosure, and at least two cyber attacks on South Korea. As for non-state actors, 'Anonymous' hacker group, famous from 2008 due to attack on Church of Scientology website, was active in Singapore. The alleged reason behind the attack was protest against a new law on media. Also, the so-called 'largest publicly announced DDoS attack in the history of the Internet.'[19] took place in March.

Some of most prominent stories from 2014 include Dragonfly cyber espionage campaign, that targeted defence and aviation companies from US, Canada and European Union, and Sony Pictures hack that exposed both employees' personal information and unreleased films details, reportedly performed by North Korean hackers in retaliation of company's plans to film a comedy about North Korean leader [20].

Important events of 2015 included the US Office of Personnel Management (OPM) attack, that had far-reaching consequences. For example, a piece of news by CNN [21] suggests

that after US government employee sensitive data was stolen, a number of CIA workers were pulled back from the US embassy in China.

2016 saw interference in US presidential election and Brexit vote, as well as two allegedly state-sponsored attacks on Yahoo that compromised half a billion and billion accounts respectively[22].

Year 2017 was marked by numerous attacks on businesses (Deloitte, HBO, Vevo), with attack on a consumer credit reporting agency Equifax making headlines as 'one of the largest data breaches in the United States' [23] . Many attacks were ransom oriented: attackers targeted schools in the US, threatening to release information unless paid [24], Uber paying hackers not to disclose data breach [25], the NotPetya, WannaCry, and Bad Rabbit ransomware cases also being prominent examples. The US National Security Agency (NSA) data breach, reported the same year, was described as worse than Ed.Snowden leak. As one of the consequences, three malware products (NotPetya, WannaCry and Bad Rabbit) used the leaked tools developed by NSA. Similar to email leak in wake of US Presidential elections of 2016, in 2017 Emmanuel Macron's election campaign in France was under attack.

If attacks reported in 2017 were numerous, those of 2018 appear game-changing. Cambridge Analytica scandal revealed powerful information warfare strategy, and cyber attack tool LoJax, also known as UEFI rootkit or hackers 'Holy Grail', was found in use for cyber espionage in Balkans, Central and Eastern Europe. Bloomberg 'Big Hack' story suggested an unprecedented supply-chain attack. Later same year, Mariott hotel chain database with personal information of around 500mln. guests was compromised, attributed to Chinese espionage effort related to earlier data breaches. This story may suggest how previous, 'long forgotten' information leaks can build up into a serious leverage over time.

Table 1. Prominent cyber and information security breaches

Year Actor	State	Non-state
2013	Jan: The New York Times hacking attempt blamed on China; -Mar: South Korea media and banking attack; -Jun: South Korea government website hack; -Jun: Israel accuses Iran of non-stop attacks on computer systems.	- Mar: "the largest publicly announced DDoS attack in the history of the Internet." -Nov: 'Anonymous' group Singapore hack.
2014	- Mar: Ukraine accuses Russia of compromising mobile network; -Jul: Dragonfly cyber espionage discovered; -Nov: Sony Pictures hack; -Nov:US Post hacked; -Nov: Regin spyware discovered; -Dec:South Korea nuclear plant compromised; - Dec: Kenya arrests 77 Chinese citizen accused of running a cybercrime center.	-Jun: World Cup in Brazil threats by 'Anonymous' group.
2015	-Feb: SIM cards producer company Gelmato hack; -Feb: alleged cyberattack on Sony Pictures Entertainment by North Korea; -Jun: German parliament cyber attack; - Jun: US federal employees data breach (the 'OPM' hack).	-Jan: US military social media hacked by ISIS sympathizers.
2016	-Mar: Petya malware; -US presidential election: - Jun: The Democratic National Committee files exposed; - Dec: US Department of Homeland Secutrity accused of trying to access state of Georgia election databade. -Jul: Russian Federal Security Service reports a "professional" cyber attack; - Sep and Dec: 'State-sponsored' attacks on Yahoo; - Dec: FBI investigates FDIC hack.	-Aug: 'Shadow Brokers' group claims to have stolen US NSA data.
2017	- Apr: US NSA breach; - May: WannaCry ransomware attack discovered, hitting 150 countries; - May: Emmanuel Macron's data leak in wake of French election; - Jun: NotPetya ransomeware attacks major companies;	-Jul: Equifax credit bureaus breach; -Sep: Attack on U.S. Securities and Exchange Commission; -Oct: Hackers target schools threatening to release private records unless paid.

	-Jun: US voters information leak; -Oct: Bad Rabbit ransomware (mainly Russia and Ukraine); -Dec: the plants in the Middle East were stopped by a Triton malware attack.	
2018	-Mar: Cambridge Analytica scandal (US and Nigeria election); -Mar:Russian Government Cyber Activity Targeting Critical Infrastructure Sectors; - Sep: UEFI Rootkit LoJax ("the hackers' Holy Grail") discovered in use; - Oct: Bloomberg 'Big Hack' story; - Dec: Marriott hotel chain database compromised	-Feb: Olympic Destroyer' malware attack confirmed; -Jan: India national database with citizen biometrical data stolen.

Source: systemized by athors based on [19-28]

Trends in connectivity, technology and geopolitics

To understand latest developments in connectivity, we look at «Measuring the Information Society» report by International Telecommunication Union [26], and «Use of Internet Services» report by European Commission, 2018.

The ITU report states that Internet usage keeps growing, with more than a half of world population online by the end of 2018 (51,2%, or 3.9 billion people). Developed countries are reaching saturation (about 80% of population online), while the developing countries still have a room to catch up (only about 45% online). The European Commission reports a moderate increase in use of social networks (reaching 65% of users) and reading news online, that can give a slowly increasing leverage for propaganda in EU.

It is obvious that amounts of data being produced will grow exponentially. However, all the data - accompanied by AI analysis - creates new threats to information security. For example, AI tools allow to create very persuasive 'deep fake' videos, contributing to blurring lines between fake and reality.

As for ***geopolitical trends***, we look into "The Global Risks Report 2019" by World Economic Forum [28]. The report points out at erosion of global cooperation, and pervasiveness of idea of 'taking back control'. Political tension between major powers were rising in 2018, and the survey showed pessimistic about 2019 developments. Changes in US-China relations, and differences in fundamental values are among key factors.

4. Review of existing categorizations of threats to cyber and information security

Analysing existing literature on the topic, we look into classifications, taxonomies and categorizations alike. Although the material on the topic is abundant, and the attempts to categorize the attacks dates back at least to 1990s [29], we haven't found the classifications of cybersecurity threats specifically tailored for a thread to a state in international relations.

Many papers on the topic target private sector organizations, or at best offer an approach that incorporates threats related to public sector. Some target specific topics - such as critical infrastructure [30-32] , automotive vehicles [33] or look into attacks in a particular sector [34].

As for the state and interstate agencies, there are two categorizations we're aware of: EUROPOL's taxonomy and UK National Cyber Security Center categorization. However, both of them were not designed for threat analysis in international relations [35-37].
With that being said, and given that there is no suitable classification that we are aware of, a set of related literature from three disciplines was reviewed:

Computer science (cyber threat/risk taxonomy, taxonomy of cyber attacks)
Legal (taxonomy of cybercrime)
Political science

Literature in each of this categories has it's advantages and disadvantages. For example, computer science classifications, developed for cybersecurity professionals, can be too technical and they often target private sector organizations. Law taxonomies can be more helpful. They have a higher degree of abstraction and can focus on 'human' side, for example intention behind cyberattack. Developed for law enforcement, it may have details excessive for our purposes, too. Political science would fit best, however there is lack of resources on the topic. In this category, we looked at three books: "World Order" by Henry Kissinger [38] , Schmidt, Cohen "The New Digital Age"[39] and "The World Hybrid War", Horbulin [40] .

Computer science
The most extensive source on the topic cyber threats we've encountered is «Systematic Review: Cybersecurity Risk Taxonomy» by Rea-Guaman et al.[41]. The review investigates publications made between 1990 and 2017 found at IEEE Explore, Science Direct, ACM Digital Library and Web of Knowledge. The authors claim to have found 132 papers during the search, however identified only 14 as relevant.

Nine primary studies identified in the paper confirm lack of generalized classification of cyber threats applicable to international relations. The studies concern specific sectors, environments or needs, and do not present a holistic approach to cyber threats.

'A Review on Taxonomies of Attacks and Vulnerability in Computer and Network System' by Joshi, Singh and Tarey, looks into taxonomies starting from as early as 1970-s [42]. Unlike the previous review, it lists the works devoted not to cyber risks, but to attacks and vulnerabilities. Many of the sources analyzed are too technical, meaning they present technical details that are redundant for the purposes of our analysis. Two classifications were of interest for our enquiry. First one is classification by Kjaerland, 2006 [42]. It consists of four categories - method of operations, impact of the intrusion, source of the intrusion, and target. We will use this categorization later for our analysis, in a modified form.

Second one is AVOIDIT, of year 2009 [43]. It is a five-dimensional classification, and the components are Attack Vector, Operational Impact, Defense, Informational Impact and Target. The advantage of this topology is that it allows for classification of blended attacks. Although four components of the taxonomy do not apply for our purposes, one of the AVOIDIT components is interesting for our enquiry - namely the classification by Information Impact. It has five parts: Distort (modifying information), Disrupt (makes target unable to provide services), Destruct (deletion of information), Disclosure (unauthorized access to information) and Discovery (gathering data in the system).

Another source used is MITRE ATT&CK matrix of cyber attack tactics and techniques [44]. MITRE is a non-for-profit organization that manages US federal research and development centers. The matrix includes 11 categories, encompassing 114 techniques of attack. This source was useful since it gives an overview of existing attacks, and helps to check if a categorization encompasses the majority of modern threats.

Legal

As Li [45], points out in literature review on the topic of cybercrime taxonomy in law, «an exhaustive bibliography is neither necessary nor possible». However, we review three sources: Li [45], Jahankhani et al.[46] and Yar [47].

The classifications analyzed in literature review by Li [45] (Bequai, Wasik, Grabosky) all have limited application for developing political cyber threats categorization. They include irrelevant categories like cyber vandalism, cyber money laundering, financial theft, etc. Nevertheless, the classifications have applicable categories, too - for example, theft of information, political and industrial espionage. Li's classification uses data processing systems as a central concept. Based on it, the work presents the following classifications of offences in which data processing systems: are targeted, are used as instruments, act as mass media, act as a transfer channel, appear as crime scenes, act as operating mechanism, are used in preparation for other crimes.

Moreover, the work presents a classification of relevant conceptions: white-collar crime, economic crime, corporate crime, professional crime and transnational crime. Here, transnational crime refers to the crimes where offenders are located in other country, and does not refer to cyber warfare component.

Valuable is a remark about category of actions that are 'not uniformly regarded as cybercrime' - namely, the physical attacks on electronic systems (for example, cutting Internet cables). It's understandable why the debate exists in law (it's a question weather to include it into 'traditional' or 'cyber' categories), and why the computer science is not interested in it (it has little to do with computer science). However, we opt to include this into our categorization. The reason is that this kind of attacks can cause severe implications, and can be a tool of hybrid warfare.

Work "Cyber crime Classification and Characteristics" by Jahankhani et al.[46], cites classifications of Yar, Gordon and Ford. However, those are not suited for the purposes of our enquiry.

However, the paper includes The Matrix of Cybercrime by Wall, 2005. It has three categories: more and new opportunities for traditional crime, and new opportunities for new types of crime.

These categories can be transformed for the purpose of hybrid threads in warfare analysis, cyber attacks that create:

- more opportunities in traditional warfare;
- new opportunities in traditional warfare;
- new opportunities for new types of warfare.

Similar idea stands behind classification into cyber-enabled and cyber-dependent crimes. However, we prefer the three-component classification as more extensive.

Book "Cybercrime and Society" by Yar, 2013, has a related chapter called "Political hacking: from Hacktivism to Cyberterrorism" [47, p. 44-62]. Although it does not present cyber attacks as a tool in relations between states, it can be useful for developing a perspective on non-state actor behavior, especially on terrorism. The chapter cites the forms of hacktivism, discusses definitions of cyber terrorism and common attack scenarios. Those are:

- attack on power system;
- disruption of financial system;
- bringing transportation system to a halt;
- stealing top-secret information.
- It also lists forms of Internet-enabled terrorist activities, including:
- communication and coordination;
- propaganda, publicity and recruitment;
- information gathering
- fundraising and financing.

Political science

"World Order" by Henry Kissinger, 2014 edition [38], contains chapter on cybersecurity under name "Cyber Technology and World Order". Summarizing, we can distil the factor of how environment has changed and what is the new threat landscape. The fundamental properties of current state of cyberspace are:

- fast growth of computation power (Moore's law);
- instantaneous connectivity;
- large part of human activity is now "quantifiable and analizable";
- governments moving its operations "into digital domain".
- The risks we can distil from the chapter are as follows:
- threats are hard to define and attribute;
- intelligence capabilities are enhanced;
- attack from a single small actor can have far-reaching consequences;
- lack of international dialogue on cyber offence can be a threat to international order.

Moreover, the chapter acknowledges information security (in meaning presented in this paper), mentioning psychological manipulation:

"The emphasis of many strategic rivalries is shifting from physical to information realm, in the collection and processing of data, the penetration of networks, and the manipulation of psychology".

On the same topic, Schmidt and Cohen in 'The New Digital Age', talk about propaganda and disinformation, mentioning they "have always been central features of human conflict". However, authors claim that 'marketing wars' (e.g. imposing narrative) will be integral part of conflicts, and refer to retaliation in cyber attacks.

"The World Hybrid War: Ukrainian Forefront" [40] by the scholars of Ukrainian National Institute of Strategic Studies, describes hybrid warfare techniques used by Russian Federation against Ukraine. It is useful as a source of information abou such threats as fake news and propaganda, and helps to determine the interplay between traditional and cyber methods in hybrid conflict. In particular, section 2.2, "Media Support of Hybrid War", describes in detail how news and social media compliment Russian effort.

Proposed categorization

The literature review didn't show a classification or topology suitable for the purposes of our research, at least in its original form. For this reason, a need to compose a categorization of threats for cybersecurity and information security arises.

Our categorizations was inspired by Kjaerland, 2006, as described in the literature review by Joshi, Singh and Tarey [42], and "The Hybrid Threat Modeling Method" blog post of April 23, 2018, by Nancy Mead and Forrest Shull, Carnegie Mellon University Software Engineering Institute [48].

As already mentioned, the paper uses cyber intrusion categorization based on four categories: method of operations; impact of the intrusion; source of the intrusion; target.
Modifying this approach, we suggest to change the meaning of the categories, leaving the structure almost untouched. The new categories are:

- By cyber-physical medium - *cherchez la technologie*

As a rule of thumb, we assume that anything connected to the Internet, or, more specifically, anything that has some kind of computational unit in it, can be compromised and become subject to cyber attack. "At present, we can roughly assert that the whole data processing systems are targets" [45]. The physical mediums have been chosen because no software and no data production, collection or manipulation can exist without hardware. The downside of this category is that it cannot be described extensively. Nevertheless, we can leave this category as descriptive for the purpose of further analysis.

- Impact - what kind of damage can be done

After analyzing the mediums of attack (laptops, smartphones, smart watch) we can look at how an intruder can actually benefit from getting access to those electronic systems. Getting access to classified information distributed inside of the system (e.g. Ghostnet, or

Sony attack in 2015), controlling the physical devices on the network (like, for example, Stuxnet changed the speed of centrifuges rotation), or purely Distributed Denial of Service (DDoS) attacks (e.g. during Russia-Georgia war in 2008 [49]) can all be examples of such damage. For this part of categorization, we used a part of above mentioned taxonomy by EUROPOL ("Common Taxonomy for Law Enforcement and CSIRTs"), and AVOIDIT taxonomy [43].

- Source of the intrusion - who are the actors

The 'warfare' part of cyberwarfare could belies the variety of actors that can be involved. Not only nation states, but also non-state actor should be accounted for.

- Target - who is under attack

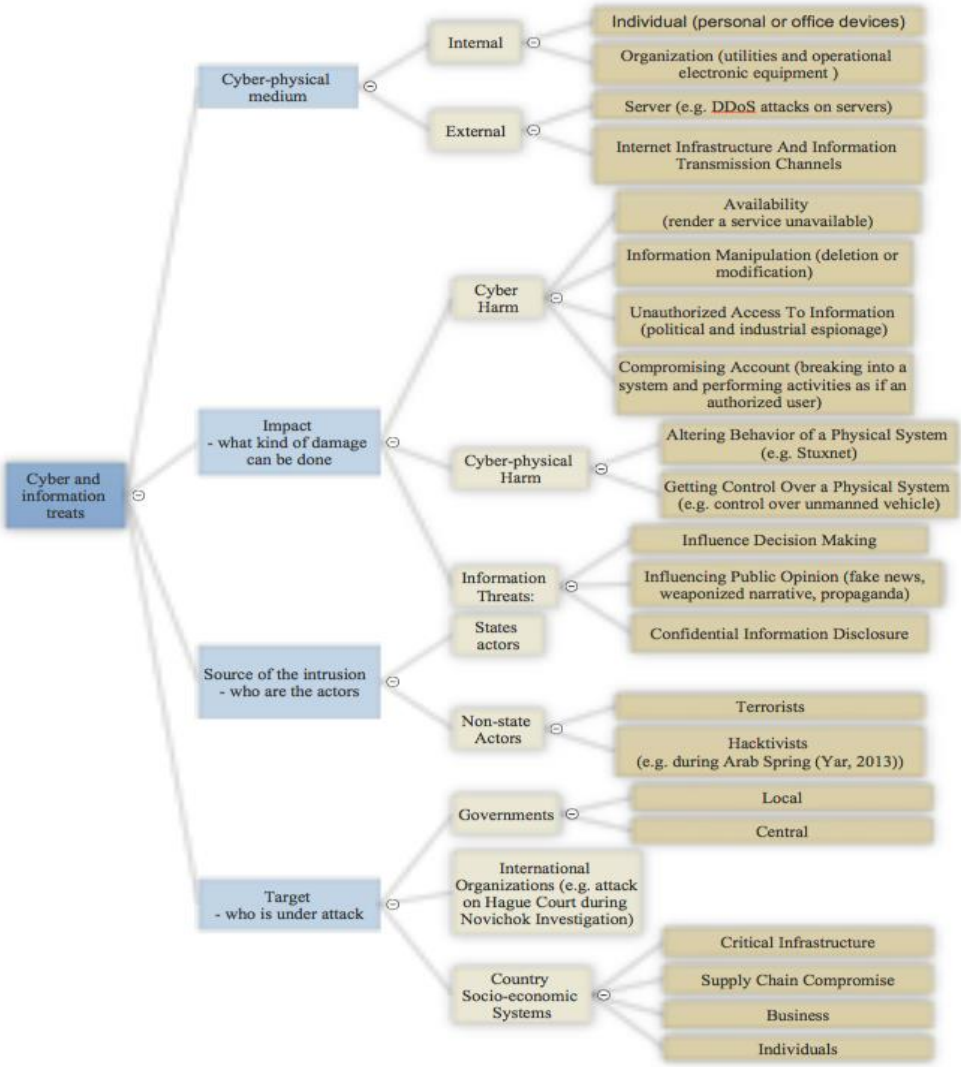

Fig. 1. Categorization of Cyber and Information Threats
Source: developed by authors

To see a thread landscape more clearly, it's useful to dissect the specific sectors and systems that can be under attack (e.g. state agencies, local governments, critical infrastructure). We include business and individuals into the list, and explicitly mention the financial sector among critical infrastructure. The reason is the fact that intellectual property theft through business espionage, compromising stability of financial sector or influencing opinions through fake news or 'troll factories' can all be considered modern threats to cybersecurity and information security.

The full classification shown in Fig 1.This categorization, although may not be extensive, reflects the variety of threats to cyber and information security. It can be used for analysis thereof and to see the wider picture of hybrid threats. For example, analysis be cyber-physical medium can be effective to identify new threats: critical infrastructure control systems - once there are any electronic control systems - can be subject to attack. Advances in the IoT can engender new threats to international cybersecurity by providing new mediums.

5. Hybrid nature of modern threats to cyber and information security

In this part, we analyse how the phenomena associated with cyberspace relate to conventional threats and practices. By exploring its 'hybrid nature', we try to elaborate how the phenomena compliment, enhance or change the 'host' system.

Defining hybrid threats

There is an extensive use of hybrid threats notion in NATO and EU resources. However, no standard definition of the concept has been adopted - and probably the ever-changing nature of the issue is both an explanation and a rationale behind it [50] . As a result, the definitions are predominantly descriptive.

An early example from 'BI-SC Input for a New NATO Capstone Concept for The Military Contribution to Countering Hybrid Threats'[51], describes the threats quite broadly as '*those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives*'.

More recent and deeper description was provided in Joint Communication To The European Parliament And The Council on Joint Framework on countering hybrid threats, [52]: *"While definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats."*

European Union External Action Service factsheet [53] is the most recent source encountered. However, it predominantly consists of description that resembles the Joint Framework mentioned above.

Same as The Joint Framework, the factsheet indicates that hybrid risks are not limited to 'traditional' cyber attacks, but also include influencing social dynamics*: 'Hybrid threats can range from cyberattacks on critical information systems, through the disruption of critical services such as energy supplies or financial services, to the undermining of public trust in government institutions or the deepening of social divisions.'*

Thus, this definition implicitly includes the notion of information security in wider understanding as defined earlier ("undermining of public trust in government institutions or the deepening of social divisions").

By summarizing above mentioned, we can assert that while unified hybrid threats definition has not yet been developed, threats to cyber and information security constantly appear in the descriptions of the notion as a part of wider scope of hybrid threats.

Types of hybrid threats in cyber and information security

A number of practices emerge in the intersection of international relations and cyberspace:

- Cyber leverages to diplomacy;
- Retaliation for cyber attacks;
- Cyber sabotage and espionage;
- Propaganda;
- Cyber troops, weapons and arm race.

Cyber leverages to diplomacy

Questions of cyber and information security can manifest themselves in diplomacy in a number of ways. First and most obvious is cyber intelligence. Second is the cyber attack attribution. Public attribution is a specific tool that can indicate the state of relations between states. The decision depends widely on the will of an affected actor since there is rarely a certainty about the attack source, and there are ways to retaliate through different channels and inform an opponent privately, without publicly announcing it. Making investigation of cyber attacks public can also serve as a kind of deterrence technique, informing the opponent that serious measures can be undertaken, and the kind if behavior will not be tolerated. Joint statement by United Kingdom Prime Minister Theresa May and Dutch Prime Minister Rutte of October 2018 on 'the unacceptable cyber activities of the Russian military intelligence service' can serve as an example of a more decisive charge: 'Our action today reinforces the clear message from the international community: We will uphold the rules-based international system, and defend international institutions from those that seek to do them harm.' [54].

State reaction to possible supply chain risks posed by foreign companies can be another tool. For example, with introduction of 5G technology in 2018, three of Five Eyes intelligence alliance countries blocked Chinese company Huawei from supplying the equipment for the technology [55].The reasoning behind this is a possibility of espionage

or disruption of the network in the future. However, the United Kingdom decided not to ban the company - possibly trying to preserve economic ties with China with view to a potential economic aftermath of Brexit.

Another leverage is international cyber crime investigations and extradition of cyber criminals. International cooperation on this issue shows many successful examples, however some states may exhibit reluctance: 'In some instances, nations shield their citizens from the rule of law with schemes that waste resources, cause needless delay, thwart investigative efforts, and undermine justice' as US Department of Justice Deputy Attorney General pointed out at the Interpol General Assembly of November, 2018 [56].

Yet another concern is misunderstanding non-state actors may cause in international cyber relations. Rise of 'cybercrime-as-service' and availability of leaked tools developed by governments can make the problem of attribution even more challenging, as hackers either work 'freelance' for interested groups, or at least have the tools to make influence themselves, if politically motivated. For example, an attack on a news agency in Qatar in 2017 and subsequent spread of fake news on its behalf led to a diplomatic crisis in the region [57]. The possibilities cyberspace offers to non-state actors, combined with predicted rise of Internet services use in developing countries, increased ability to conceal the source of attack and persisting global instabilities, suggest that more attacks are likely to take place and destabilize fragile balances in conflict areas and undermine state sovereignty.

Retaliation for cyber attacks

Another practice often observed in cyberspace is retaliation - a deterrence tactic, or possibly an excuse for action. As noted in report by Kaspersky Lab in 2019, 'In terms of retaliation for instance, governments might use them as a response ranged somewhere between a diplomatic answer and an act of war, and indeed some governments are experimenting with them.'[58]. The practice can be both cyber and non-cyber. For example, the United States imposing new sanctions on North Korea in 2015 [59] in retaliation of attack on Sony Pictures is a non-cyber action, while unusual banking hack of 2013 is believed to be Iran's retaliation for US sanctions and cyber attacks - namely Stuxnet[60].

The persistence of the retaliation practice can be explained by relatively low cost of the attack and constant uncertainty about opponent's behavior. Reputation costs are low, too - although they went higher, since countries tend to take more harsh position on the issue. Weak protection in cyber pace makes defence strategy less rewarding and pushes players into attack-as-a-defence field.

Cyber sabotage and espionage

While some vectors of cyber attacks may change over time, espionage effort and compromising data constantly make headlines. The threat can be seen as 'cyber-enhanced', since new means only complement long-established practices. However, the amount of data available is new, and the outreach is unprecedented.

The examples of cyber sabotage include rendering government websites unavailable, disruption of critical infrastructure operation (for example, Stuxnet), or even revealing unpublished movie scripts during Sony Picture attack. In the field of information security, making data of The Democratic National Committee public during US presidential election of 2016, and leak of Emmanuel Macron's data in wake of French presidential election in 2017 can be regarded as sabotage.

Cyber espionage, pervasive both in interstate relations and business, can be considered as constant long-term threat. Espionage effort can be also an effective counter-intelligence measure. For example, CNN suggests that after sensitive data about US government employees was stolen in 2015, a number of US Beijing embassy workers in were pulled back from the US embassy in China [61].

Propaganda

Another 'cyber-enhanced' tool is propaganda. The attempts to influence adversary's (or ally's) opinion is nothing new - however, has ever it been so effective. Today, the efforts are equipped with information - gathered by intelligence or publicly available - and advanced means to analyse it.

Of course, the interference in US election and Brexit vote [62], both as Russian efforts in Ukraine, were not solely done by the means of Internet. However, the events have shown how effective such medium-term manipulations can be. The promises of the tools like Cambridge Analytica, troll factories and fake news entail a number of consequences.

First, the tools are likely to be applied widely - both in conflict areas, during the axises of geopolitical tensions and, most importantly, during key political events. Upcoming European Parliament Elections, Ukrainian election in March 2019 and Canadian federal election in October 2019 are a few recent events likely to be affected.

Second, there is still a question on to what extent can the 'foreign government' propaganda influence national opinions. So far, it has been efficient in influencing matters where the opinions were divided. However, there is still a question if propaganda can effectively change the dominating narrative. A shift like this would probably need a long-term effort - and thus it raises a question of protection from this kind of influence.

Cyber troops, weapons and arm race

Cyber and information security means can be described differently. For cyber security, they are equipment, computer programmes and units that are used to compromise adversaries computer systems. For information security units we take definition of cyber troops by Oxford Computation Propaganda Research Project Working Paper no.2017.12: 'Cyber troops are government, military or political party teams committed to manipulating public opinion over social media' [63]. Information security weapons include programmes and algorithms of analyzing data reinforced by AI as well.

As there is actors' adaptation and catch-up of techniques in the domain of conventional weapons, the same is true for cyber and information weapons. While this kind of 'field

levelling' happens in every domain of human activity, it can lead either to predictable developments connected to resource accumulation ('cyber arm race'), or to show new, previously unthinkable way of attack, challenging the established conventions ('open a pandora box'). Precisely, we can say that cyber weapons started a race, yet information threats rather opened a pandora box, making security as an ecosystem worse off and making attack landscape appear even more gruesome.

An intersection of cyber war and conventional war comes in treating cyber weapons like conventional weapons. This includes more control over it's flow, for example through custom regimes. An attempt was made in 2014, changes to the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ('Wassenaar Arrangement') were made to include certain types of software, specifically the ones exploiting 'zero-day' vulnerabilities [64]. The Wassenaar Arrangement is a multilateral export control with 42 members as of February 2018, including the US, majority of EU countries, Russia, India, Japan and South Korea. The move was advocated by the need to keep the software away from repressive regimes and cyber criminals. However, the Wassenaar Arrangement is not legally binding.

The set of threats described as 'hybrid' calls for a need to cope with a gargantuan amounts of information available both to allies and adversaries, and the need to analyse this data in various ways. However, no problem comes without a solution: amplified data supply comes hands in hand with advances in computational power and information processing methods. Rise of AI is yet another method to help navigate complex data landscape.

The drive of countries to equip themselves with the most efficient cyber weapons is natural. However, this drive may push the governments into cooperation with cyber criminals. Accompanied by growth of crime-as-a-service, hiring hackers for a specific task, or recruiting them long-term can become increasingly pervasive practice. It's likely to see next election, with political opponents hiring hackers to compromise one another.

6.Conclusion

Spread and wide use of the Internet - something unexpected yet influential, making it one of Nassim Taleb's 'black swans' - apparently caught the world off-guard. Politics, law and security have not yet came up with a matching response.

And yet, the lack thereof is understandable - technology is still a 'boiling pot', with the active 'tectonic plates' drift. Increase in computation power and data storage capabilities is yet to reach a plato, and data analysis tools like artificial intelligence have not yet shown their full potential. Humanity has not yet familiarize themselves with all the possibilities the new tool offers, and will apparently come up with numerous new uses and misuses.

Governments came up with different responses, and defined cyber security and information security in different ways. While US, EU, and NATO have defined the notions strictly, the Russian definition is more vague, allowing to classify the information flows the government perceives as unfriendly as a threat to information security. However, this definition does not contradict to the one by US-EU-NATO - yet it is broad enough to match

information security as a security in information warfare (disinformation, expectation management, etc.), although giving disproportionate power to government. In our paper, we referred to information security in this wider sense, namely incorporating the psychological component and the social consciousness.

Doctrines on information security is a modern policy are being developed in response to hybrid threats (Ukraine) or with offencive aim (Russia), both in information space and in a physical world. Although the need to address the challenges posed by information threats in wider meaning of the term is apparent, existing practices, like blocking ideological content in information space, cannot be considered as the best way to address the issue, and should be negotiated by civil society and lawmakers. Hence, the best practices for combating this kind of threats are yet to be developed.

Within last five years (2013-2018), the attacks increased in sophistication and impact, building upon the experiences and leaks from the past. Every year the news stories are reporting some 'unprecedented' or 'worse then ever' breaches, meaning attackers' imagination is not as nearly matched by appropriate safeguards.

After analysing cyber threat and related notions classification in computer science, law, and political science, we did not find the classification or topology that we could use to describe cyber security threats from a point of view of international relations, and extend to incorporate a notion of information security. Unable to find categorization of threats to cyber and information security in literature, we offered a categorization consisting of four parts - by cyber-physical medium, by impact - what kind of damage can be done, by source of the intrusion - who are the actors, and by target - who is under attack.

Hybrid nature of modern threats to cyber and information security manifests itself in diplomacy, sabotage and espionage effort, propaganda and arm race. It also gives rise to the practice of cyber retaliation. Cyber leverages to diplomacy evolve around gathered intelligence information, allowing actors to maneuver through decisions on publicly blaming a state for a cyber attack, economic leverages (e.g. precluding actors with close ties to a foreign government from entering the market), and cooperation on international cyber crime investigations. However, a chance of misattribution - both an advantage and a threat - can lead to destabilization, especially if level of trust between actors is low. The problem aggravates once non-state actors with access to leaked state tools come into equation.

Retaliation for cyber attacks is a practice that can be done both be cyber and non-cyber means. The persistence of the retaliation practice can be explained by relatively low price of the attack in terms of reputation and costs, and constant uncertainty about opponent's behavior.

Cyber offence may be more effective than cyber defence, but keeping advantage in offence can be harder than with conventional arms since cyber 'weapons' are easier to replicate and adopt. Leaks of information from state agencies only adds to the 'levelling the field'. An

intersection of cyber war and conventional war comes in treating cyber weapons like conventional weapons.

References

[1]Schwab, Klaus. 2017. *The Fourth Industrial Revolution*. London: Penguin Random House.
[2]Case, Steve. 2016. *The Third Wave*. New York: Simon & Schuster.
[3]Abramson, Bram Dov. 2006. "Word Matters: Multicultural Perspectives On Information Societies - By Alain Ambrosi, Valérie Peugeot, & Daniel Pimienta". *Journal Of Communication* 56 (3): 627-628. doi:10.1111/j.1460-2466.2006.00305.x.
[4]Bartsch, Michael, and Stefanie Frey. 2018. *Cybersecurity Best Practices : Solutions To Increase Cyber Resilience For Businesses And Government*. Springer-Verlag.
[5]Cyber Security Strategy Documents". 2019. *CCDCOE*. https://ccdcoe.org/cyber-security-strategy-documents.html.
[6]"Security And Prosperity In The Digital Age: Consulting On Canada's Approach To Cyber Security". 2019. *Publicsafety.Gc.Ca*. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-scrty-prsprty/index-en.aspx.
[7]"National Cyber Security Agenda | NCSC". 2019. *Ncsc.Nl*. https://www.ncsc.nl/english/current-topics/national-cyber-security-agenda.html.
[8]2019. *Hcpn.Gouvernement.Lu*. https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/national-cybersecurity-strategy-3/national-cybersecurity-strategy-iii-en-.pdf.
[9] "X.1205: Overview Of Cybersecurity". 2010. *Itu.Int*. https://www.itu.int/rec/T-REC-X.1205-200804-I.
[10] "Law Of Ukraine "About The Basic Principles Of Ensuring Cyber Security Of Ukraine"". 2019. *Cis-Legislation.Com*. http://cis-legislation.com/document.fwx?rgn=101792.
[11] "Information Security Doctrine Of The Russian Federation September 2000 | Public Intelligence". 2000. *Publicintelligence.Net*. https://publicintelligence.net/ru-information-security-2000/.
[12]"Doctrine Of Information Security Of The Russian Federation". 2016. *Mid.Ru*. http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.
[13]"President Approved Information Security Doctrine Of Ukraine — Official Website Of The President Of Ukraine". 2017. *Official Website Of The President Of Ukraine*. https://www.president.gov.ua/en/news/glava-derzhavi-zatverdiv-doktrinu-informacijnoyi-bezpeki-ukr-40190.
[14]"Cyber Security Strategy Of Ukraine". 2016. *Ccdcoe.Org*. https://ccdcoe.org/sites/default/files/documents/NationalCyberSecurityStrategy_Ukraine.pdf.
[15]"1834: The First Cyberattack - Schneier On Security". 2018. *Schneier.Com*. https://www.schneier.com/blog/archives/2018/05/1834_the_first_.html.
[16]Jacobsen, Jeppe Teglskov. 2014. "The Cyberwar Mirage And The Utility Of Cyberattacks In War How To Make Real Use Of Clausewitz In The Age Of Cyberspace". *Diis.Dk*. https://www.diis.dk/files/media/publications/import/extra/diis-wp_2014-06_teglskov_web.pdf.
[17]"The 20 Most Infamous Cyberattacks Of The 21St Century (Part I)". 2015. *MIT Technology Review*. https://www.technologyreview.com/s/540786/the-20-most-infamous-cyberattacks-of-the-21st-century-part-i/.
[18]Thornburgh, Nathan. 2005. "Inside the Chinese Hack Attack". *TIME.com*. http://content.time.com/time/nation/article/0,8599,1098371,00.html.
[19] Markoff, John, and Nicole Perlroth. 2013. "Firm Is Accused Of Sending Spam, And Fight Jams Internet". *Nytimes.Com*. https://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html.
[20]Peterson, Andrea. 2014. "The Sony Pictures Hack, Explained". https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?noredirect=on&utm_term=.e0aa2f00c422.
[21]Perez, Evan. 2015. "U.S. Pulls Spies From China After Hack". *CNN Money*. https://money.cnn.com/2015/09/30/technology/china-opm-hack-us-spies/.
[22]Nicole Perlroth, Vindu Goel. 2016. "Yahoo Says 1 Billion User Accounts Were Hacked". Nytimes.Com. https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.
[23]"Equifax Hackers Steal Personal Details Of Up To 143 Million People". 2017. Fortune. http://fortune.com/2017/09/07/equifax-hackers-personal-details-143-million-people/.

[24]Larson, Selena. 2017. "Hackers Are Targeting Schools, U.S. Department Of Education Warns". *CNN Money*. https://money.cnn.com/2017/10/18/technology/business/hackers-schools-montana/index.html?iid=EL.
[25]Wong, Julia. 2017. "Uber Concealed Massive Hack That Exposed Data Of 57M Users And Drivers". *The Guardian*. https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack.
[26]"Measuring The Information Society Report 2018". 2018. *Itu.Int*. https://www.itu.int/en/ITU-D/Statistics/Pages/publications/misr2018.aspx.
[27]"Use Of Internet And Online Activities - Digital Single Market - European Commission". 2018. *Digital Single Market - European Commission*. https://ec.europa.eu/digital-single-market/en/use-internet.
[28]"The Global Risks 2019. 14th Edition". 2019. weforum.org. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.
[29]Hansman, Simon, and Ray Hunt. 2004. "A Taxonomy Of Network And Computer Attacks".*Ants.Iis.Sinica.Edu.Tw*.
http://ants.iis.sinica.edu.tw/3bkmj9ltewxtsrrvnoknfdxrm3zfwrr/17/attacks%20taxonomy.pdf.
[30]Fleury, Terry, Himanshu Khurana, and Von Welch. "Towards a taxonomy of attacks against energy control systems." In International Conference on Critical Infrastructure Protection, pp. 71-85. Springer, Boston, MA, 2008.
[31]Zhu, Bonnie, Anthony Joseph, and Shankar Sastry. "A taxonomy of cyber attacks on SCADA systems." In 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing, pp. 380-388. IEEE, 2011.
[32]Miller, Bill, and Dale Rowe. "A survey SCADA of and critical infrastructure incidents." In Proceedings of the 1st Annual conference on Research in information technology, pp. 51-56. ACM, 2012.
[33]Sheehan, Barry, Finbarr Murphy, Martin Mullins, and Cian Ryan. "Connected and autonomous vehicles: A cyber-risk classification framework." *Transportation Research Part A: Policy and Practice* (2018).
[34]Radmand, Pedram, Alex Talevski, Stig Petersen, and Simon Carlsen. "Taxonomy of wireless sensor network cyber security attacks in the oil and gas industries." In *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, pp. 949-957. IEEE, 2010.
[35]Kiwia, Dennis, Ali Dehghantanha, Kim-Kwang Raymond Choo, and Jim Slaughter. "A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence." *Journal of computational science* 27 (2018): 394-409.
[36]"Common Taxonomy For Law Enforcement And Csirts". 2017. *Europol*. https://www.europol.europa.eu/publications-documents/common-taxonomy-for-law-enforcement-and-csirts.
[37]"New Cyber Attack Categorisation System To Improve UK Response To Incidents - NCSC Site". 2018. *Ncsc.Gov.Uk*.
https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents.
[38]Kissinger, Henry. *World order*. Penguin Books, 2014.
[39]Schmidt, Eric, and Jared Cohen. *The new digital age: Reshaping the future of people, nations and business*. Hachette UK, 2013.
[40]Horbulin, Volodymyr. "The world hybrid war: Ukrainian forefront." *Kharkiv: Folio* (2017).
[41]Rea-Guaman, A. M., T. San Feliu, J. A. Calvo-Manzano, and I. D. Sanchez-Garcia. "Systematic Review: Cybersecurity Risk Taxonomy." In International Conference on Software Process Improvement, pp. 137-146. Springer, Cham, 2017.
[42]Joshi, Chanchala, Umesh Kumar Singh, and Kapil Tarey. "A review on taxonomies of attacks and vulnerability in computer and network system." *International Journal* 5, no. 1 (2015).
[43]Simmons, Chris, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, and Qishi Wu. "AVOIDIT: A cyber attack taxonomy." In Proc. of 9th Annual Symposium On Information Assurance-ASIA, vol. 14. 2009.
[44]"MITRE ATT&CK™". 2019. Attack.Mitre.Org. https://attack.mitre.org/.
[45]Li, Xingan. "Taxonomy of Cybercrime." *Journal of Legal Studies* 1, no. 1 (2016): 1-27.
[46]Jahankhani, Hamid, Ameer Al-Nemrat, and Amin Hosseinian-Far. "Cybercrime classification and characteristics." In Cyber Crime and Cyber Terrorism Investigator's Handbook, pp. 149-164. 2014.
[47]Yar, Majid. *Cybercrime and society*. Sage, 2013.
[48]Mead, Nancy R., Forrest Shull, Krishnamurthy Vemuru, and Ole Villadsen. "A Hybrid Threat Modeling Method." (2018).
[49]White, Sarah. 2018. "Understanding Cyberwarfare: Lessons From The Russia-Georgia War - Modern War Institute". *Modern War Institute*. https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/.

[50]"Joint Framework On Countering Hybrid Threats A European Union Response." 2016. *Hybridcoe.Fi*. https://www.hybridcoe.fi/wp-content/uploads/2017/08/Joint-Framework-on-countering-hybrid-threats-1-2.pdf.
[51]"Bi-SC Input To A New NATO Capstone Concept For The Military Contribution To Countering Hybrid Threats." 2010. *Act.Nato.Int*. http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf.
[52]"Joint Framework On Countering Hybrid Threats A European Union Response.", 2016
[53]"A Europe That Protects: Countering Hybrid Threats - EEAS - European External Action Service - European Commission". 2018. *EEAS - European External Action Service*. https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en.
[54]"Joint Statement From Prime Minister May And Prime Minister Rutte". 2018. *GOV.UK*. https://www.gov.uk/government/news/joint-statement-from-prime-minister-may-and-prime-minister-rutte.
[55]"Why Has The UK Not Blocked Huawei?". 2018. *BBC News*. https://www.bbc.com/news/technology-46370014.
[56]"Deputy Attorney General Rod Rosenstein Delivers Remarks At The Interpol 87Th General Assembly". 2018. *Justice.Gov*. https://www.justice.gov/opa/speech/deputy-attorney-general-rod-rosenstein-delivers-remarks-interpol-87th-general-assembly.
[57]"Qatar-Gulf Crisis: Your Questions Answered". 2017. *Aljazeera*. https://www.aljazeera.com/indepth/features/2017/06/qatar-gulf-crisis-questions-answered-170606103033599.html.
[58]"Kaspersky Security Bulletin: Threat Predictions For 2019". 2019. Media.Kasperskycontenthub.Com. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/11/27082929/KSB_Predictions-2019_General-APT.pdf.
[59]"U.S. Targets North Korea In Retaliation For Sony Hack". 2015. *The Wall Street Journal*. https://www.wsj.com/articles/u-s-penalizes-north-korea-in-retaliation-for-sony-hack-1420225942.
[60]"Bank Hacking Was The Work Of Iranians, Officials Say". 2013. *The New York Times*. https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.
[61]"U.S. Pulls Spies From China After Hack". 2015. *CNN Money*. https://money.cnn.com/2015/09/30/technology/china-opm-hack-us-spies/.
[62]"Signs Of Russian Meddling In Brexit Referendum". 2017. *The New York Times*. https://www.nytimes.com/2017/11/15/world/europe/russia-brexit-twitter-facebook.html.
[63]Howard, Phillip, and P. Bradshaw. "Troops, trolls and troublemakers: a global inventory of organized social media manipulation." (2017): 1-37.
[64]Granick, Jennifer. 2014. "Changes To Export Control Arrangement Apply To Computer Exploits And More". *The Center For Internet And Society, Stanford Law School*. http://cyberlaw.stanford.edu/publications/changes-export-control-arrangement-apply-computer-exploits-and-more.