©LUMEN Proceedings

2nd International Conference Global Ethics -Key of Sustainability (GEKoS) | May 14, 2021 | Bucharest, Romania

Ethics in Cyberspace – Dangers and Threats

Denisa-Atena COSTOVICI (MEMA)

https://doi.org/10.18662/lumproc/gekos2021/6

How to cite: Costovici (Mema), D.-A. (2021). Ethics in cyberspace – dangers and threats. In A. Grigorescu & V. Radu (vol. ed.), *Lumen Proceedings: Vol. 15. 2nd International Conference Global Ethics - Key of Sustainability (GEKoS)* (pp. 71-83). Iasi, Romania: LUMEN Publishing House. https://doi.org/10.18662/lumproc/gekos2021/6

Ethics in Cyberspace – Dangers and Threats

Denisa-Atena COSTOVICI (MEMA)[1]

Abstract

Rapid technology development and easy access to virtual space was directly proportional to the proliferation of multiple categories of network users and consumers. This contemporary reality has contributed to the emergence of the illusion of unrestricted accessibility of the online environment and the permissiveness of expression "no matter what". The cyberspace draws a thin line between freedom of expression and violation of behavioural norms toward others. In order to mitigate the behaviours that transcend ethical boundaries, a series of basic conditions of use and restrictions have been legislated (mainly crimes related to threats and illegal content shared in the virtual world) which do not include all the situations encountered in practice. Given the cyberspace dimension, prevalent in most civilized areas of the planet, as a means and method of intercultural communication, ethical standards should be standardized and applied uniformly. This research paper is an attempt to objectively address the issues of standards and ethical values on the Web, with reference to cyber terrorism, groups of organized crime, hacktivism and states' implication and responsibility. The main hypothesis of the research emphasizes that the information society requires the creation and enforcement of new laws, because it coexists in a completely new environment - the Network. Referring to the Network links, it is a fact that it cannot be kept safer against unauthorized access, without the application of adequate security measures and techniques. This research paper aims to shed the light on the dangers and threats that challenges the information society thought cyberspace.

Keywords: *cyber threats, cyber-attack, cybercrime, security, cyberspace.*

[1] National University of Political Studies and Public Administration, Bucharest, Romania, E-mail: denisa21co@gmail.com

1. Introduction

Towards the end of the twentieth century, society began to explore and exploit an artificial, man-made environment - cyberspace. Our daily lives, fundamental rights, social interaction and the world economy depend on information and communication technology that works on the basis of the Internet. The free and open virtual environment has promoted global political and social inclusion, opened up barriers between countries, communities and citizens, enabling interaction and the exchange of information and ideas around the world.

This new environment for the propagation of power presents numerous opportunities for economic, cultural or technological development, which has favoured a mass transition to the online environment. However, cyberspace is an insecure environment. Each of the levels which compose cyberspace - physical infrastructure, operational software, information and not in the least people – can be the target of breaches, either as a result of an attack or by infiltration or by accident.

By exploiting vulnerabilities in the computer systems, a cyber-attack can jeopardize the security of critical infrastructure. Vulnerabilities result from the weaknesses of the technology and due to the improper implementation and supervision of technological products. The human factor can also be a generator of risks and vulnerabilities by underestimating the severity of threats or poor implementation of security policies and procedures (Constantin et al., 2020). Although hard to believe, cybercriminals rely primarily on people to follow the steps that get the malware installed or to redirect resources and information for them. There have been made numerous attempts of creating an effective scale that records aspects of individual compliance with cyber security protocols. The permeability of individuals to security procedures is an important aspect in assessing the vulnerabilities of an organization or company, influencing its cyber security.

States have begun to develop information infrastructures and adopt strategies to regulate the activity of individuals and legal entities, to ensure that citizens' rights are respected and to prevent the spread of cybercrime in the virtual world (Borţea, 2020). Cybersecurity has gradually become a major concern for decision-makers, who want to neutralize risks and counter potential attacks in cyberspace.

In this research paper we will analyse the ethics applied on the mode of action in cyberspace, more precisely on the phenomena and threats existing in the virtual environment.

2. Problem Statement

A fundamental issue for the decision maker is the manner in which an appropriate balance should be struck between the revaluation on the positive aspects of the online environment against accepting the risks that may appear as a result. In other words, an upper level of functionality often leads to increased vulnerability - namely, the multiplication of the number of sites expands Internet access and utility, but in the same time increases the probability of malware being downloaded to someone's computer. In order to make an assessment of this kind, the risks and the repercussions must be assessed - both in the short and long term.

In addition to the facilities that the internet and interconnectivity provide us, the virtual world can hide unknown or difficult to foresee threats from users (Pruteanu, 2020)[13].

The choice of a research topic aimed at ethics in cyberspace is based on the fast pace of development of information and communication technology, which tilts the balance towards increasing the number of cyber-attacks and aggressors, and therefore the difficulty of assigning and designing response mechanisms.

During the research it was found that in the literature predominates the concept of "cyber-attack" defined as "hostile action carried out in cyberspace likely to affect cybersecurity", to the detriment of "cyber threat".

Strategic documents sought to formulate a definition that encompasses the specific features of this type of threat. An example is Romania's Cyber Security Strategy in which the cyber threat is described as "a circumstance or event that may generate a potential danger to national security" and is characterized by asymmetry, increased dynamics, global character and diversity (National Association for the Security of Information Systems, 2012, p. 24).

In this sense, the two notions, "cyber-attack" and "cyber threat", are interconnected in the following manner: a cyber-attack represents an offensive action, while a cyber threat refers to the probability of materialisation of a certain attack. Cyber-attacks are classified from the perspective of the Romanian Intelligence Service (in order of importance for national and international security) as follows:

• state (most often cyber espionage),

• cybercrime (carried out by more or less structured crime groups, organized or not),

• ideologically motivated (activism in the online environment – hacktivism (Romanian Intelligence Service, 2019) and, respectively, cyber terrorism).

It is difficult to predict the modus operandi of a cyber attacker, but by analysing the case, cybersecurity companies compile statistics and trends that can guide the efforts of decision makers to strengthen cyber resilience.

The perpetrators of cyber-attacks differ in terms of knowledge, skills, motivations and resources. These features are used to identify their targets, what data or infrastructure is of interest to them and in which way they will perform cyber-attacks. The most frequent perpetrators of cyber-attacks are:

I. State actors

Cyber threats that are attributed to state actors have the greatest impact on national security. Governments, aware of the advantages and dangers generated by and in cyberspace, are mobilizing their resources to pursue "politics through other means," as Clausewitz defined war in the cyberspace. Nowadays, governments actively capitalize on "hackers" in order to achieve their strategic goals - defending their own infrastructure, economy and other assets, using deterrence as their first line of defence (von Clausewitz, 2006).

State cyber-attacks present relatively low risks unlike traditional military and espionage operations. The process of assigning a cyber-attack is very difficult, and the accusation of a state requires solid evidence, difficult to obtain in an environment as volatile and dynamic as cyberspace.

Cyber-attacks carried out by state actors mainly target strategic government areas, such as national defence and security, the energy sector, foreign affairs, economics or research, etc. Cyber-attacks against a state usually "hit" institutions, ministries, embassies or private companies of strategic interest.

II. Hacktivist groups

The concept "hacktivist" was coined in 1994 by a group of hackers formed in 1984 in Lubbock, Texas called Cult of the Dead Cow (CDC). Hacktivism includes civil disobedience transposed into cyberspace, representing a new type of threat. The concept of hacktivism is found at the convergence of two terms hacking and activism, where "hacking" is used to refer to operations that exploit computer systems / networks in illegal ways, usually with the help of special designed software. While activism is defined as "a non-destructive use of the Internet for ideological purposes," hacktivism uses hacking tools to promote ideals and causes disruptively, but not seriously or violently. The cyber-attacks used by these groups do not require advanced knowledge, they are not very complex. The most common types of cyber-attacks used are website defacement, Denial of Service

attacks, information theft, website parody, virtual sabotage and software development.

III. Terrorist groups

The threat posed by this phenomenon has attracted the attention of the media, the security community and the IT industry. Terrorism is a politically motivated act and therefore requires publicity and an audience to which the messages transmitted should be reflected. The main actions through which the cyber environment is exploited by terrorist groups are propaganda, recruitment, radicalization, communication and research (Kalakuntla et al., 2019).

Romania's cyber security strategy defines this category of cyber actors as: "terrorists or extremists who use cyberspace to carry out and coordinate terrorist attacks, communication activities, propaganda, recruitment and training, fundraising, etc., for terrorist purposes". The Romanian Intelligence Service nuances the characteristics of this phenomenon, proposing the following definition: "activities carried out in cyberspace, by people, groups or organizations motivated extremist-terrorist (ideological or religious), in order to support recruitment, radicalization, propaganda and funding (cyber-enabled-terrorism), or for conducting cyber-attacks against IT&C (cyber-dependent-terrorism) systems that can cause material destruction or casualties."

Cyber-terrorism is certainly a convenient option for modern terrorists, who are attracted by the advantage of anonymity, the possibility of causing massive damage, the psychological impact on the population and visibility.

IV. Cybercrime groups

The relevance of these attacks to national security is medium as the financial and digital economy areas are the main targets. Cybercriminals want access to personal, financial or health data - to monetize it on underground black markets. These markets are dispersed, diverse and segmented, growing and constantly changing to keep pace with consumer trends, but also to prevent law enforcement and national security bodies from understanding them. They come in many forms. Some are dedicated to a specialized product or service. Others offer a range of goods and services to carry out a complete cycle of a cyber-attack - from the tools needed to operate a system, attack infrastructure, malware, maintenance, to cyber laundering services for stolen goods.

Cyber-attacks by organized crime groups are largely profit-oriented and pose a significant and global threat. These cyber-attacks target access to the financial resources of the targeted users, but also data to sell them, hold them for ransom or to exploit them in another way, the main purpose being all financial accumulation. Cybercriminals can work on an individual base or in groups to obtain their goals.

Cybercrime covers any illegal conduct through electronic operations aimed at the security of computer systems and the data they process. In a broader sense, they cover any unlawful practices committed through or in connection with a computerized network or system, counting offenses such as illegal possession and provision or distribution of information through a computer system or network (Gordon & Ford, 2006).

Cybercrime groups are also involved in sophisticated ransomware attacks. Terms such as hacking, malware, botnets, phishing, which had only emerged

in the past few years, became items of common parlance as the frequency of cyber-attacks launched by cybercriminals in various domains from governments to business sector and individual level. Characteristic to these crimes is the fact that they exceed all borders and are a serious threat to all users

3. Aims of the research

It is of high relevance to analyse the application of ethics standards in the virtual environment, a world that fascinates us and in which we are increasingly immersed. The scientific approach will follow to what extent the threats present in the cyberspace can influence the whole information society and is going to draw the coordinates of cybersecurity as an emerging dimension of national security, as evidenced by the literature and strategic documents. Creating a strategic framework for cybersecurity requires a thorough understanding of the cyberspace, the relations between the main actors, but also the knowledge of the capabilities and intentions to carry out cyber-attacks.

This paper aims to discuss some aspects of cybersecurity, namely to analyse the dynamics and risks posed by the emergence of cyber threats in society, as a result of violating ethical standards. During the paper will be presented the types of cyber threats, the actors and the area on which their impact is reflected.

4. Research Methods

The thematic analysis of the phenomenon of cyber threats represents the principal methodology utilized in this study.

The documentation included the interconnected concepts of cyber-attack, cyber threats and cyber security. Through direct observation, the main actors of cyber threats were analysed, with emphasis on their motivation, modus operandi and the degree of impact of actions.

The presented data was collected through the empirical study. Thus, attempts to legislate cybercrimes were noted, the case study being applied to Romania. The research has shed the light on measures of resilience against cyber-attacks adopted by states - entities with authority in the field.

5. Findings

In the past, the worst threats to the security of a state were undoubted the enemy troops amassed at the border. In the present, the paradigm has changed. The last 20 years have been marked by an explosion of new threats both nationally and internationally. Internal and collective security mechanisms have faced new security threats. The emergence of non-state actors, for example terrorist groups or drug cartels intra- state conflicts are among the current threats.

The emergence of several non-state actors, such as terrorist networks or drug cartels and intra-state conflicts are among the current threats. The revolution brought by the development of information and communication technology (ICT) favoured the intensification of cyber threats, triggering the slow transition from traditional battlefields - ground, air and sea - to cyberspace.

Cyber security is a cross-cutting issue that permeates all aspects of a modern society and economy, and this makes it difficult to identify the problems and measures needed to counter them. Cyber security is not limited to network and information security. It covers any illegal activity that implies actions conducted in the cyberspace, being the result of a gear of actions and resources, which involves the prevention, detection, reaction and return after cyber incidents.

There is no standard, universally accepted definition that encompasses all aspects of this dimension. Cyber security is a complex subject and has been characterized over time by several definitions.

One of them is the one formulated by the "National Initiative for Cybersecurity Careers and Studies" (NICCS), which presents the above-

mentioned concept as: “the activity, process, capacity or state through which information and communication systems and the information contained in them are protected against damage, unauthorized use or modification or exploitation”. CISCO proposes the following definition of cyber security: "cyber security is the practice of protecting systems, networks and programs against digital attacks". This definition boils down to the defensive dimension, emphasizing proactive measures, building a protective shield that must be available at all times. This state of alert that the companies send to users can be explained by the rapid technological evolutions that favour the permanent appearance of new threats to which we must adapt.

Cyber security has also become a topic of interest for Romania, joining states around the world in trying to regulate the most dynamic and difficult-to-manage dimension of national security.

In Romanian doctrine, cyber security is described as “the state of normalcy resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity and non-repudiation of information in electronic format, public resources and services or private, from cyberspace”.

The 21st century has suggestively acquired the name "information age", in which citizens can have much easier access to a variety of information. However, the rapid developments recorded in the ICT field have led to impressive changes in the way information is used, modifying the manner in which it is used or stored by both civilian population and state institutions. Cyber-attacks and information exploitation became two of the most frequent and feared threats to national security, and just like the physical plan, both offensive and defensive actions take place in this new arena - the virtual one.

All these new threats to the national security of a state go beyond the scope of traditional threats in terms of complexity and asymmetric character. As Joseph Nye and David A. Welch have stated, the global scene is becoming more and more congested and the dynamics of the international stage witnesses the emergence of non-states actors. Consequently, the difficulty to face these threats increase and the rules of the games start to fade (Nie & David, 2013, pp. 201-214).

Cyber security issues are caused by three factors that act simultaneously:

- the presence of actors with hostile intentions in the cyberspace;
- the company's dependence on ICT for many important functions;
- the inevitable presence of vulnerabilities in ICT systems.

In cyberspace, the vectors of threat can be cybercrime organizations, hackers, terrorists or state actors, hereinafter referred to as

cyber actors. They could steal personally identifiable information (PII) to engage in illegal activities hosted by the virtual world, which has the potential to transform each individual in a victim. If a state is victim of a cyber-attack the consequences fall over the population and the values protected by the respective state, the threat may be to the entire state and its values.

A cyber threat has the potential to spread very quickly to all levels of society based on the speed with which actions are produced and propagated in an increasingly interconnected world. States remain the central figure that has the authority and capabilities to address cyber threats, as they remain the strongest actors in the international system.

In recent decades, the cyber threat has become one of the most persistent and dynamic threats against national security, including Romania, both quantitatively, given the number of cyber-attacks and the complexity of the methods involved. Since 2007, many countries have explicitly included cyber threats in their national security strategies. Recognizing the vulnerabilities inherent in a digitalised and interconnected society is a first proactive measure to counter these threats. States need flexible and dynamic cyber security strategies to respond to cyber threats in an ever-changing and developing environment, such as cyberspace (Costovici et al., 2020). Romania's national defence strategy for the period 2015-2019 also included cyber threats, and since 2013, major steps were taken in this matter as a cybersecurity strategy was drawn alongside a national action plan which provided the base of the National Cyber Security System.

In Romania, there are a number of crimes sanctioned through the Criminal Code (2020), CHAPTER VI - Crimes against the security and integrity of computer systems and data, Articles 360-336 - art. 360 "Illegal access to a computer system, Unauthorized transfer of computer data", art. 361 – "Illegal interception of a computer data transmission", art. 362 – "Alteration of computer data integrity", art. 363 – "Disruption of the functioning of information systems", art. 364 – "Unauthorized transfer of computer data", art. 365 – "Illegal operations with computer devices or programs", as well as: Art. 230 – "Unlawful use of another's communication terminal or use of a communications terminal connected without right to a network, if a damage has occurred", art. 249 – Computer fraud, Art. 311 – "Counterfeiting of credit titles or payment instruments", art. 314 – "Possession of instruments for counterfeiting values", art. 325 - Computer forgery, art. 374 - Child pornography, art. 388 – Fraud at electronic voting, art. 391 – Forgery of electoral documents and records.

Without realizing it, we are constantly exposed to threats in the virtual environment through the constant use of the Internet, but we are not

aware of the impact that these threats would have on us. Although security incidents and cyber-attacks are becoming more frequent, we have not yet adopted prudent conduct regarding the activity carried out in the virtual environment.

Cyberspace is the new dimension in which people have expanded their activity. Similar to land, sea, air or space, there are resources, interests and, inevitably, conflicts in cyberspace. As well as organizations make use of all technologies available to create effects in other operational areas, people do the same. The economy, industry, administration are sectors of activity that have focused on this dimension, becoming the targets of cyber-attacks. The constituent elements of cyberspace are inherently vulnerable to a wide range of cyber-attacks. The dynamism, anonymity and connectivity specific to cyberspace are favourable factors for cyber-attacks.

The analysis of the dynamics of cyber-attacks shows a significant increase in the frequency, intensity, duration and complexity of cyber-attacks. The general perception is that organizations and companies are primarily targets of cyber-attacks, but at the individual level there is the same probability of being a victim of cybercrime. Statistics derived from these types of attacks reported in January 2020 show that cyber-attacks on people rank third, after the administrative and industrial sectors, with a share of 12.3% (Passeri, 2020).

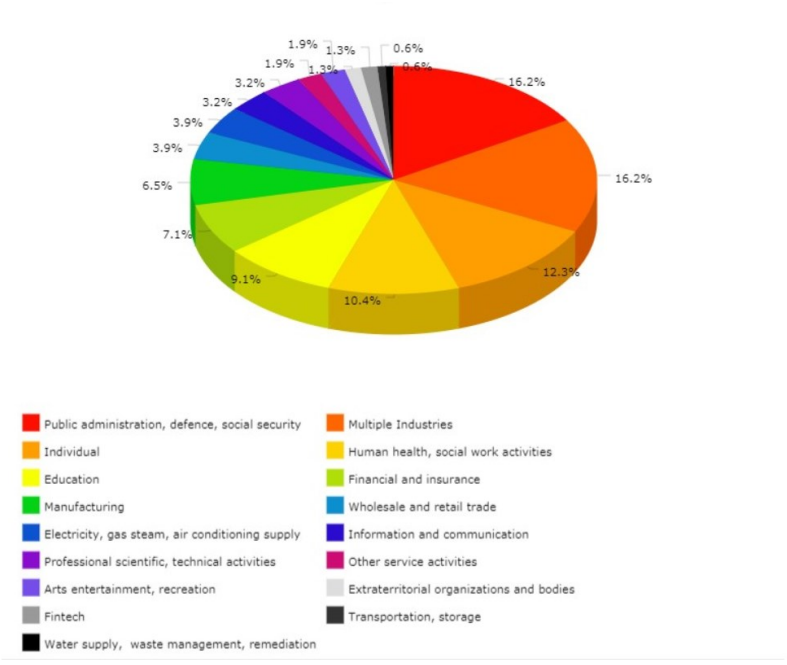

Figure 1. Targets of cyber-attacks. Source: Passeri (2020)

6. Discussions

Information technology has become ubiquitous and irreversibly integrated into society. Cyber threats are the most current and versatile threats to national security. If at the beginning of the 21st century, they were in the realm of emerging security challenges, now cyberspace has become an environment for the spread of strategic interests. Cyber threats are different from conventional threats in that their effects are visible in both the virtual and physical environment. Their effects can be immediate or programmed for an opportune moment, being difficult to detect without specific capabilities. The resonance of these threats in the strategic plan is based on two major considerations: they harm national values and interests and cause financial losses (Andrei[Martin], 2016, p. 14).

In a digital world, cybersecurity has become very important for companies, agencies or government organizations, as well as for individual users (Pascal, 2021). As early as the beginning of the 21st century, we witnessed a rapid technological evolution that led to the reconceptualization of the notion of security, and implicitly to the emergence of a new subdomain of it - cyber security. Improving the level of cybersecurity with a strong accent on the protection of critical infrastructure are essential measures that can affect the general level of security and economic well-being.

An overview of the dynamics of the global cyber threat landscape indicates a significant spike of the intensity, frequency, duration and sophistication of cyber-attacks, especially in recent decades. Mostly, cybersecurity issues stem from the inherent nature of information technology (IT), the complexity of information systems, and improved attackers' skills and capabilities.

In addition, cyber threats to national security are evolving. As new ways of counteracting appear, vectors adapt by developing new tools and techniques to compromise security. As innovation produces new applications for information technology, new places are emerging for criminals, terrorists and other hostile parties, along with new vulnerabilities that cyber actors can exploit. States need to develop and strengthen mitigation and resilience strategies to deal with large-scale attacks.

References

Andrei (Martin), I. (2016). *Managementul Securităţii Cibernetice la Nivel Naţional* [Cyber Security Management at National Level] [Summary of Doctoral dissertation,"Alexandru Ioan Cuza" Police Academy Bucharest] https://www.academiadepolitie.ro/root/studii/iosud/rezumate_teze/2016/martin/rezumat_teza_andreimartin.pdf

Borţea, A. N. (2020). The Ethics of Public Administration in the Digital Economy. In A. Grigorescu & V. Radu (vol. ed.), *Lumen Proceedings: Vol. 11. 1st International Conference Global Ethics -Key of Sustainability (GEKoS)* (pp. 254-263). Iasi, Romania: LUMEN Publishing House. https://doi.org/10.18662/lumproc/gekos2020/26

Constantin, M., Borţea, A. N., & Costovici, D. A. (2020). Risks and Vulnerabilities in Digital Public Services. Threat of Cyberterrorism Vs Romania's Cybersecurity Strategy. *HOLISTICA Journal of Business and Public Administration, 11*(2), 74-84. https://doi.org/10.2478/hjbpa-2020-0020

Costovici, T., Panait, C., & Pisargiac, C. (2020, March 4). *Evolutia reglementarilor din domeniul securitatii nationale* [Evolution of regulations in the field of national security]. Romanian Intelligence Magazine. https://intelligence.sri.ro/evolutia-reglementarilor-din-domeniul-securitatii-cibernetice/

Gordon, S., & Ford, R. (2006). On the Definition and Classification of Cybercrime. *Journal in Computer* Virology, *2*(1), 13-20. http://dx.doi.org/10.1007/s11416-006-0015-z

Kalakuntla, R., Vanamala, A. B., & Kolipyaka, R. R. (2019). Cyber Security. *HOLISTICA Journal of Business and Public Administration*, *10*(2), 115-128. http://doi.org/10.2478/hjbpa-2019-0020

National Association for the Security of Information Systems. (2012). *Cod de bune practici pentru securitatea sistemelor informatice şi de comunicaţii* [Code of good practice for the security of information and communication systems]. https://www.cert.ro/vezi/document/cod-bune-practici-securitate-it-2015

Nye, J. S. Jr, & David, A. W. (2013). *Understanding Global Conflict and Cooperation: An Introduction to Theory and History*. Pearson.

Pascal, R. (2021, May 24). *Awareness in era digitală* [Awareness in the digital age.] Romanian Intelligence Magazine. https://intelligence.sri.ro/awareness-era-digitala

Passeri, P. (2020, March 3). *January 2020 Cyber Attacks Statistics*. HACKMAGEDDON.https://www.hackmageddon.com/2020/03/03/january-2020-cyber-attacks-statistics/

Pruteanu, S. M. (2020). Ethics – A Mandatory Instrument to Ensure Good Governance of the Public Sector. In A. Grigorescu & V. Radu (vol. ed.) *Lumen Proceedings: Vol. 11. 1st International Conference Global Ethics -Key of Sustainability (GEKoS)* (pp. 316-327). Iasi, Romania: LUMEN Publishing House. https://doi.org/10.18662/lumproc/gekos2020/32

Romanian Criminal Code. (2020). Law 286/2009. https://legeaz.net/noul-cod-penal/art-360

Romanian Intelligence Service. (2019, September 19). *Glosar de termeni pentru domeniul Securitatii Cibernetice* [Glossary of terms for the field of Cyber Security]. https://www.sri.ro/assets/files/publicatii/GLOSAR-TERMENI-CYBER-12-09-2019.pdf

von Clausewitz, C. (2006). *On War.* (J. J. Graham, Trans.) E-book retrieved from https://www.gutenberg.org/files/1946/1946-h/1946-h.htm.