SJIF Impact Factor: 6.260| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 5 | Issue: 3 | March 2020 - Peer Reviewed Journal

CYBER THREATS AND VULNERABILITIES

Ўринов Нодирбек Тохиржонович
Анджанский государственный университет

Сайидова Нигора Комилджоновна
Анджанский государственный университет

Юлдашев Хушнидбек Дилмурад ўғли
Анджанский государственный университет

ABSTRACT

This chapter describes and evaluates the cyber world, including its phenomena, from a strategic perspective. As no universally accepted definitions for the cyber world exist, associated literature and publications address it in many different ways. A five-layer model is constructed for cyber threats, which include cybervandalism, cybercrime, cyber intelligence, cyberterrorism and cyberwarfare.

This chapter depicts the standards-based risk model, cyber operations and cyberweaponry, as well as the critical structures of society as the targets. Moreover, cyber security definitions are provided. Cyber world phenomena are addressed in more detail in other chapters of this book.

1.1 CYBER THREATS

Threats to society's vital functions may directly or indirectly target national systems and/or citizens, from within or outside the national borders. The threat landscape is a list of threats containing information about threat agents and attack vectors. By exploiting weaknesses/vulnerabilities, threats may lead to a loss or takeover of assets. The threats to society's vital functions can be divided into three entities which are: physical threats, economic threats and cyber threats.

Physical threats include:

- Natural disasters (e.g. earthquake, tsunami, volcanic eruption, flood).
- Environmental disasters (e.g. nuclear fallout, oil spill, toxic chemical discharges).
- Widespread technical disruptions (especially those in ITC systems).
- Conventional warfare with kinetic weapon systems.
- Terrorist strikes with kinetic weapon systems, and
- Civil unrest (violence, sabotage).

Economic threats include:

- Deep national depression.
- Deep global depression.
- Disruption in national or global financing markets, and
- Sudden global shortage of goods and services.

Threats in cyberspace can be classified in many ways. The threat landscape is a list of threats containing information about threat agents and attack vectors. By exploiting weaknesses/vulnerabilities, threats may lead to a loss or takeover of assets.

The European Network and Information Security Agency (ENISA) uses a cyber threat model consisting of threats. The threats include different forms of attacks and techniques as well as malware and physical threats. In the ENISA-model "a threat agent is any person or thing that acts (or has the power to act) to cause, carry, transmit, or support a threat". Some of the major threat agents in cyberspace are corporations, cybercriminals, employees, hacktivists, nation states, and terrorists (ENISA 2012b).

SJIF Impact Factor: 6.260| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 5 | Issue: 3 | March 2020 - Peer Reviewed Journal

One of the common threat models is a fivefold classification based on motivational factors: cyber activism, cybercrime, cyber espionage, cyber terrorism and cyber warfare. With a typology such as this motives can reduced to their very essence: egoism, anarchy, money, destruction and power. This fivefold model is derived from Myriam Dunn Cavelty's structural model (Cavelty 2010; Ashenden 2011).

Level 1 consists of cyber activism which encompasses cyber vandalism, hacking and hacktivism. For a single company or an individual their activities can cause significant economic losses. The recent activities of the Anonymous hackers have been more effective than in the past.

Level 2 consists of cybercrime. The Commission of the European Communities defines cybercrime as "criminal acts committed using electronic communications networks and information systems or against such networks and systems" (Commission of the European Communities 2007).

Level 3 consists of cyber espionage. This can be defined as action aimed at obtaining secret information (sensitive, proprietary or classified) from individuals, competitors, groups, governments and adversaries for the purpose of accruing political, military or economic gain by employing illicit techniques in the Internet, networks, programs or computers (Liaropoulos 2010).

Level 4 consists of cyber terrorism which utilizes networks in attacks against critical ICT systems and their controls. The purpose of the attacks is to cause damage and raise fear among the general public, and to force the political leadership to give into the terrorists' demands (Beggs 2006).

Level 5 cyber warfare consists of three separate entities: strategic cyber warfare, tactical/operational cyber warfare and cyber warfare in low-intensity conflicts. No universally accepted definition for cyber warfare exists; it is quite liberally being used to describe the operations of state-actors in cyberspace. Cyber warfare per se requires a state of war between states, with cyber operations being but a part of other military operations.

The threats to society's vital functions can also simultaneously occur in each of the three abovementioned dimensions. For example, cyber operations and action aimed at collapsing an adversary's economy can be included in conventional warfare. When it comes to terrorism, different operations in the cyber world and the economic system can be included in strikes that cause physical destruction.

Disruptions can impact and escalate across the dimensions. For instance, a natural disaster can cause widespread disruptions in the power grid, which may adversely affect the operation of payment systems and the food distribution chain. When prolonged, they may result in civil disturbances.

1.2 CYBER ACTIVISM

Cybervandalism and hacking saw the light of day in January 1985 when two Pakistani brothers released *Brain,* the first computer virus developed for the pc environment. Hacking was the pursuit of amateurs until 2000, when professionally coded malware began to pop up in the network environment. The first spyware appeared in the mid-2000s, targeting the weapons industry, governments and NGOs, among others. The discovery of the computer worm *Stuxnet* in 2010 heralded a new dawn as regards malware. Stuxnet, co-created by the United States and Israel, was discovered as it was spreading in Europe, India and the Middle East. It was rumoured to contain up to 20 zero-day exploits. Within 25 year hacking, originally an amateur activity, matured into state-run information warfare in global networks and systems (Hypponen 2010).

Hactivism stands for the different forms of computer and online activism, mostly on the Internet. The term was coined by conjoining the words *hacker* and *activism.* Whereas hacktivism has become a specific field of research in activism, the term itself has yet to become fully established. The reason for this is that, on the one hand, activism can tap into a range of instruments developed by hackers and, on the other hand, hackers can advance their own agenda (Hintikka 2013).

Hactivism often refers to social movements which either independently or assisted by hackers seize and utilise the possibilities offered by networks (McCaughey 2003). Jordan (2008) defines hactivism as an activity which is only possible on the Internet and exploits the manipulation of technology. In other words it relies on technological expertise. Correspondingly, hackers themselves view hacking as activism that opposes the use of technology to limit civil rights, such as Internet censorship.

Vegh (2003) divides online activism into two main categories: Internet-enhanced and Internet-based. According to him, the former concerns activism in which the Internet is mostly used as an extra communications channel or for the purpose of spreading awareness. The latter is only achievable on the Internet, just as Jordan posits.

Mobile technology and the social media offer entirely new vistas for modern cyber swarming. Harbingers of the activists' new modus operandi were in the air as early as 1998 in London and in 1999 in Seattle when groups of activists were mobilised over the Internet and led by mobile phones. Cyber swarming has assorted forms and motives. The so-called 'Botellon' gatherings, where young Spaniards socialise

SJIF Impact Factor: 6.260| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 5 | Issue: 3 | March 2020 - Peer Reviewed Journal

while drinking alcohol, are on the most benign side of the spectrum. The 2011 riots in Britain and the events associated with the Arab Spring were more serious in nature. During the British riots social media was used in organising looting and disturbances. Therefore, the UK is presently considering limitations on the use of social media in areas where riots are taking place.

In Egypt, on 25 January 2011, approximately 15,000 people gathered in the centre of Cairo for an anti-government demonstration. The organising has taken place in the social media. The next day the Egyptian leadership blocked access to Twitter and Facebook, and Internet services were almost entirely disabled on the night of Friday, 28 January. On Friday, mobile phone services were altogether discontinued in certain areas. By breaking off social communications the government aimed to prevent people from organising, preclude their situational awareness and coordination through cyber swarming. However, the measures were halfhearted and, at the end of the day, the President lost his power. Cyber swarming claimed its first notable victory.

1.3 CYBERCRIME

Commission of the European Communities defines that cyber-crime is understood as "criminal acts committed using electronic communications networks and information systems or against such networks and systems". The cyber-crime is applied to three categories of criminal activities. The first covers traditional forms of crime such as fraud or forgery, though in a cyber-crime context relates specifically to crimes committed over electronic communication networks and information systems. The second concerns the publication of illegal content over electronic media (i.e. child sexual abuse material or incitement to racial hatred). The third includes crimes unique to electronic networks, i.e. attacks against information systems, denial of service and hacking. These types of attacks can also be directed against the crucial critical infrastructures in Europe and affect existing rapid alert systems in many areas, with potentially disastrous consequences for the whole society (Commission of the European Communities 2007).

Up until a few years ago virus coding was still a young men's hobby through which they sought pleasure and acclaim among their peers. Nowadays online crime is a professional activity aimed at achieving financial gain. While the criminals rarely operate on their own, they do not necessarily form a close-knit organisation. Cooperation that resembles outsourcing is the most common practice, in which the criminals take on specific roles. A skilful programmer may code malware and sell it to a botnet operator. The operator, in turn, will sell his network services to spammers or cyber blackmailers that threaten companies with denial of service attacks. In addition, those who peddle credit card or bank account information normally prefer to sell their information, rather than use the data themselves. These complex chains make it extremely difficult to solve crime, especially when the perpetrators can be spread across the globe. Many a time the traces lead to countries whose authorities lack the will, resources or powers to solve such cases. Since the risk of being caught is negligible, online crime is an extremely lucrative business. The vast number of potential victims more than makes up for the low rate of success, or marginal profit per unit (Kaariainen 2010).

The number of cyber-attacks has dramatically increased in recent years: it has more than doubled within the past 3 years. At the same time, the financial consequences have risen by nearly 40 %. In 2011 the average annual cost for an American organisation amounted to USD 8.9 million. These days, the annual losses caused by cybercrime are close to USD 400 billion. According to forecasts, the value of solutions used in thwarting denial of service attacks keeps growing at an annual rate of 18.2 %, expected to reach USD 870 million by 2017.

1.4 CYBER WARFARE

As there is no generally accepted definition for cyber warfare it is quite liberally used in describing events and action in the digital cyber world. The concept of cyber warfare became extremely popular in 2008-2010, partly superseding the previously used concept of information warfare which was launched in the 1990s. For some, cyber warfare is war which is conducted in the virtual domain. For others, it is the counterpart of conventional 'kinetic' warfare. According to the OECD's 2001 report, cyberwar military doctrines resemble those of so-called conventional war: retaliation and deterrence. Researchers agree with the notion that the definition of cyberwar should address the aims and motives of war, rather than the forms of cyber operations. They believe that war is always widespread and encompasses all forms of warfare. Hence, cyber warfare is but one form of waging war, used alongside kinetic attacks (OECD 2001).

In the 1990s cyber warfare was associated with the concept of information warfare (IW) as its subset. Libicki (1995) defined the sectors of IW as follows:

- Command-and-control warfare, C2 W
- Intelligence-based warfare, IBW
- Electronic warfare, EW
- Psychological operations, PSYOPS
- Hackerwar
- Information economic warfare, IEW
- Cyberwar

SJIF Impact Factor: 6.260| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 5 | Issue: 3 | March 2020 - Peer Reviewed Journal

The United States defines information warfare as a range of actions taken during a conflict or war by means of information operations (IO) to achieve information superiority over an adversary. The US doctrine includes cyber operations as part of information operations. Air Force Doctrine Document 2-5 (2005) defines information operations as follows:

1. Influence Operations
   a) Psychological operations, PSYOPS
   b) Military deception, MILDEC
   c) Operations security, OPSEC
   d) Counterintelligence (CI) operations
   e) Counterpropaganda operations
   f) Public affairs (PA) operations
2. Network Warfare Operations
   a) Network attack, NetA
   b) Network defense, NetD
   c) Network warfare support, NS
3. Electronic Warfare Operations
   a) Electronic attack
   b) Electronic protection
   c) Electronic warfare support

The concept of Network Centric Warfare (NCW) emerged in American discourse at the end of the 1990s: in NCW the network gained prominence over information. The NCW concept was launched in 1998 in the US Naval Institute's publication "*Network-Centric Warfare: Its Origin and Future",* written by Vice Admiral **Arthur K. Cebrowski** (1942-2005) (Director for Space, Information Warfare, and Command and Control on the U.S. Navy staff) and **John J. Garstka**. They maintained that "For nearly 200 year, the tools and tactics of how we fight have evolved with military technologies. Now, fundamental changes are affecting the very character of war" (Cebrowski and Garstka 1998; Senenko 2007).

They went on to say that Network-centric warfare and all of its associated revolutions in military affairs grow out of and draw their power from the fundamental changes in American society. These changes have been dominated by the co-evolution of economics, information technology, and business processes and organizations, and they are linked by three themes (Cebrowski and Garstka 1998):

- The shift in focus from the platform to the network
- The shift from viewing actors as independent to viewing them as part of a continuously adapting ecosystem
- The importance of making strategic choices to adapt or even survive in such changing ecosystems.

Later the concept was published in the book *Network Centric Warfare* written by, in addition to John Gartska, **David S. Alberts** (Director, Research OASD-NII), and **Frederick P. Stein** (MITRE Corporation). According to their definition network centric warfare is "an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization" (Alberts et al. 2000).

"The term network centric warfare broadly describes the combination of strategies, emerging tactics, techniques, procedures and organisations that a fully or even a partially networked force can employ to create a decisive warfighting advantage" (Garstka 2003).

All of the abovementioned sectors need to be analysed from the offensive and defensive perspective. When it comes to IW and information operations, information is at the core of thinking. Information is seen as the fourth operational factor which glues together the three accepted operational factors: force, space and time. In IW information is understood to be data accumulation, present in any format or system, which can be utilised in communication and interaction. Furthermore, IW encompasses the following concepts: information systems, information environment, information functions and information superiority (STAE 2008).

Cyber warfare, in its present form, can be understood to incorporate both IW and EW, thereby establishing a modus operandi that complies with network centric warfare. Cyber-thinking hopes to bring the structures of cyberspace, i.e. the critical infrastructure, alongside information that is at the core of the information environment. All vital functions of society are more or less networked. Being 'networked' refers to action which is not fixed to any time or place and the management of functions. Network structures, along with information, are gaining in prominence. Yet another significant paradigm shift is the fact that while information warfare is generally perceived to occur during conflicts and war, nowadays cyber threats—in all their different forms—have become a part of everyday life for people and institutions.

Cyber warfare can be divided into strategic and operational-tactical warfare, depending on the role assigned to cyber operations in the different phases of war. State actors launch offensive cyber operations in situations where the states are not at war with each other. In this case, the cyber-attacks constitute a cyber

SJIF Impact Factor: 6.260| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 5 | Issue: 3 | March 2020 - Peer Reviewed Journal

conflict in a low intensity conflict, as was the case with Estonia in 2007.

In the spring of 2007 Estonia was subjected to a three-week long series of cyberattacks which targeted, among others, the government, the police, the banking system, the media and the business community. The cyber campaign mainly used denial of service (DOS) attacks targeting among other things web servers, e-mail servers, DNS servers and routers (Ottis 2008).

The Russo-Georgian War, also known as the South Ossetia War, was fought during the first week of August, 2008 between Georgia and the Russian Federation, and the army of the Republic of South Ossetia. In this short-lived war cyberwarfare was used as a part of conventional 'kinetic' operations. As early as 8 August several Georgian and South Ossetian websites experienced DOS attacks. The campaign against Georgian websites began on the night of August the 9th. The attacks targeted the websites of Georgia's government and President, and *Georgia-online*. On 11 August the Georgian authorities decided to fight the 'disinformation' and stopped all Russian TV broadcasts in the country. Caucasus Online, Georgia's leading Internet service provider, prevented access to all pages that had *a.ru* Internet domain suffix. The Russian *RIA Novosti* news agency's website was attacked and went down for a few hours on 10 August. The website of Russia's English-speaking TV channel *RussiaToday* was attacked on 12 August and remained inoperative for approximately 24 h. Hackers gained access to the web pages of Georgia's Central Bank and the Ministry of Defence and tampered with some media footage in them.

REFERENCES

1. *Alberts DS, Garstka JJ, Stein FP (2000) Network centric warfare: developing and leveraging information superiority, 2nd revised ed. CCRP, Washington*
2. *Arquilla J, Ronfeldt D (eds) (2001) Networks and netwars: the future of terror, crime, and militancy. RAND, Santa Monica*
3. *Ashenden D (2011) Cyber security: time for engagement and debate. In: Ottis R (ed) Proceedings of the 10th european conference on information warfare and security (ECIW 2011, Tallinn). Academic Publishing, Reading, UK, pp 11–16*
4. *Career Fields, National Security Agency, http://www.nsa.gov/careers/career_fields/*
5. *EU Commission (2009) Critical information infrastructure protection, vol 149. Brussels, COM (2009)*