SocioBrains

ISSN 2367-5721, JOURNAL HOMEPAGE: WWW.SOCIOBRAINS.COM

INTERNATIONAL SCIENTIFIC REFEREED ONLINE JOURNAL WITH IMPACT FACTOR

ISSUE 43, MARCH 2018

CYBERSECURITY AS PART OF THE CONTEMPORARY SECURITY ENVIRONMENT

Abstract: This work analyzes the main aspects of cyber security in today's extensive use of communication and information technologies (ICT). Below are the relationships between concepts such as cyber attacks, cyber warfare, cyber crime, which are the basis for the definition of cyber security. Indicated generally accepted criteria for qualitative and quantitative assessment of the importance of cyber attacks. The analyze of factors characterized the cyber stability is done, like key element, hold a priority position in security sector of the country.

Author information:

Krasimir Kostadinov
Commander(OF-4), PhD, Chief Assistant Professor,
Chair of Navy, Command and Staff Faculty
Rakovski National Defense Academy, Sofia
✉ kraspk@abv.bg
Bulgraia

Keywords:
cyberspace, cyber attack, cyber war, internet and information and communications technologies, secure routing, critical and information infrastructure.

Information technologies as part of the global internet family undergo a dynamic and intensive development in the digital and information era. Companies and state institutions rely on the cyberspace for everything – from transactions to military operations.

The Computer code blurs the line between the cyber and physical world and connects millions of objects to the Internet or private networks. The Internet is one of the fastest-growing areas of technical infrastructure development. Today, information and communication technologies (ICTs) are omnipresent and the trend towards digitization is growing. As Internet usage continues to expand, cyberspace will be increasingly dependent upon every element of our society.

The availability of ICTs and new network-based services offer a number of advantages for the society in general, especially for the developing countries. ICT applications, such as e-government, e-commerce, e-education, e-health and e-environment, are seen as enablers for development as they provide an efficient channel to deliver a wide range of basic services in remote and rural areas. Since the advent of the Internet in the 1990s not all users have acted in cyberspace for peaceful purposes. Nowadays the threat and impact of an attack in and through cyberspace has continuously grown to the extent that cyberspace has emerged as a setting for war on par with land, sea, air, and space, with an increasing potential to damage the national security.

Cyberspace is our national operating system, analogous to Windows, for example. A system crash would cause mass damage to the economy and the national security. Consequently, this paper asserts that cyber attacks can cause potentially grave damage to the national security and must be treated as an act of war.

1. Basic principles and sources of cyber warfare.

What Does 'Cyber' Mean? The word cyber is generally believed to originate from the Greek verb κυβερεω (*kybereo*) - to steer, to guide, to control. At the end of the 1940s Norbert Wiener, an American mathematician, began to use the word cybernetics to describe computerized control systems. According to Wiener, cybernetics deals with science that address the control of machines and living organisms through communication and feedback. Pursuant to the cybernetic paradigm, information sharing and manipulation are used in controlling biological, physical and chemical systems. The cybernetic system is a closed system, exchanging neither energy nor matter with its environment. [14]

As there is no generally accepted definition for cyber warfare it is quite liberally used in describing events and actions in the digital cyber world. The concept of cyber warfare has become extremely popular since 2008, partly superseding the previously used concept of information warfare which was launched in the 1990s.

To some experts, cyber warfare is war which is conducted in the virtual domain. For others, it is the counterpart of conventional ‘kinetic’ warfare. According to the Organization for Economic Cooperation and Development (OECD’s 2001 report), cyberwar military doctrines resemble those of the 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 a war, used alongside kinetic attacks (OECD 2001).

Cyber warfare, in its present form, can be understood to incorporate both information warfare (IW) and Electronic warfare (EW), thereby establishing a type of approach that complies with network centric warfare.

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, cyber-attacks constitute a cyber conflict in a low intensity conflict, as was the case with Estonia in 2007. [14]

Putting these definitions **War** and **Cyber** together, we may say that cyber war is a state of usually open, armed hostile conflict between nations, states, or parties which is related to or involving computers or computer networks.

It is clear that every modern contemporary army uses computer technologies in a certain way. Hence, every war nowadays could be regarded as a “cyber war”.

2. Cyberspace operations and cyberspace infrastructure.

Many countries are defining what they mean by cyber world or cyber security in their national strategy documents. The common theme from all of these varying definitions, however, is that cyber security is fundamental to both protecting government secrets and enabling national defense, in addition to protecting the critical infrastructures that permeate and drive the 21st century global economy. [14]

Cyberspace is a global domain within the information environment which consists of the interdependent network of information technology infrastructure, including the Internet, the telecommunications networks, the computer systems, and the embedded processors and controllers.[1]

Cyberspace is a man-made domain, and is therefore unlike the natural domains of air, land and maritime. Activities in cyberspace can allow freedom of action for activities in the other domains and activities in other domains can create effects in and through cyberspace.

The other definition of cyberspace is: “composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work”. [5]

From this definition and its implications one could deduce that cyber war is simply warfare in the cyberspace domain, but this simplification is insufficient for two reasons. ‘Warfare in cyberspace’ is too broad a definition. Dropping a bomb on a telecommunications center is not cyber war. Moreover, cyber war is not synonymous with information operations (IO), but it could be a subset of IO.

In cyberspace, a cyber attack is the mechanism that equates to the use of force.

Correspondingly the effects of cyber attack can range from mere annoyance to physical destruction and death. Cyber attacks can target individuals, objects, or entire societies. [5] Somewhere along this spectrum of conflict in cyberspace, cyber attacks cross the threshold and becomes armed attacks or operations.

Cyberspace operations – “the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the global information grid (GIG).[2]

[1] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*.

[2] JP 1-02.

Cyberspace superiority - The operational advantage in, through, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference.3

3. Potential cyber attacks and vulnerabilities to the security sector.

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. 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. earthquakes, tsunami, volcanic eruptions, floods); environmental disasters (e.g. nuclear fallouts, oil spills, toxic chemical discharges); widespread technical disruptions (especially those in ITC systems); conventional warfare with kinetic weapon systems; terrorist strikes with kinetic weapon systems; civil unrest (violence, sabotage).

Economic threats include: deep national depression; deep global depression; disruption in national or global financing markets; sudden global shortage of goods and services.

Threats in cyberspace can be classified in many ways.

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 a 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 2012). [14]

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 be reduced to their very essence: egoism, anarchy, money, destruction and power. This fivefold model is derived from Myriam Dunn Cavelty's structural model. [14]

According to the ISO 27005 definition, risks emerge from the "potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization". The risk depends on: the asset covering its business importance, existing vulnerabilities or weaknesses and the level of protection implemented through control; the threat consisting of a threat agent who - depending on their capabilities - utilizes an attack vector to compromise an asset or a set of assets. The effectiveness of an attack depends on the capability of the threat agent and the sophistication of the attack; the impact that takes into account the value that the asset represents for the business and the consequences when the confidentiality, integrity, availability or privacy of that asset is compromised though the threat.

4. NATO cyber defence policy.

NATO relies heavily on its information and computer systems to conduct operations and pass sensitive or classified data. Like many banks media or political institutions, NATO is experiencing a growing intensity and frequency of cyber attacks. Threats range from common, low-level malware to highly visible denial of service attacks or invisible but more serious attempts for cyber espionage.

Against the background of increasing dependence on technology and on the Internet, the Alliance is advancing its efforts to confront the wide range of cyber threats targeting NATO's networks on a daily basis. The growing sophistication of cyber attacks makes the protection of the Alliance's communications and information systems (CIS) an urgent task.

In order to keep abreast with the rapidly changing threat landscape and maintain a robust cyber defence NATO has adopted a new enhanced policy and its action plan, which was endorsed by Allies at the Wales Summit in September 2014. The policy establishes that cyber defence is part of the Alliance's core task of collective defence, confirms that international law applies in cyberspace and intensifies NATO's cooperation with industry. The top priority is the protection of the communications systems owned and operated by the Alliance. [8, 9]

3 Approved Air Force Space Command (AFSPC) definition of cyberspace superiority, derived from multiple AFSPC and LeMay Center cyberspace operations working groups, 2009-2010.

5. National security – Cyber challenges.

The national strategy for cyber security “Cyber resilient Bulgaria 2020”has been accepted with a Ministerial Council decision № 583 from 18th July, 2016, (valid to December 2020) and is an expression of the collective engagement and responsibility of all stakeholders and the government of the Republic of Bulgaria to ensure a modern framework and a safe environment for the development of the national system for cyber security and the achievement of an open and secure cyber space.

The vision for achieving “Cyber resilient Bulgaria 2020” outlines the development stages for the growth of the basic information security. The Republic of Bulgaria will be a reliable and resilient partner and participant in the common networks, systems and the collective security of our Euroathlantic partners, with innovative and advanced technological development meeting the priorities for the development of the economy and society, and possessing the capacity and capabilities to take part in preventing and overcoming the developing cyber threats and crises.

The strategy outlines objectives and measures in nine key areas: establishment and development of the national system for cyber security and resilience; network and information security – foundation for cyber resilience; defence and resilience of the digitally dependent critical infrastructures; improving the interaction and the information sharing between state, business and society; development and improvement of the regulatory framework; intensifying the counteraction to cyber crime; cyber defence and protection of the national security; increasing the amount of information, knowledge and competencies and developing a stimulating environment for researches and innovations in the cyber security area; international interaction – cyber diplomacy and operative interaction. The execution of objectives and targets will be developed into a Plan with a map in accordance with the planned development phases.

In conclusion, a cyber attack can cause grave damage to the national security and must be treated as an act of war. A robust international regime of laws, norms, and definitions provides the basis for deterrence in this new global, warfighting domain. The Internet is an “interconnected global network of 600 million users served by 15 million hosts connecting nearly 200 countries”. [6] Consequently, cyberspace is the world’s nervous system, the control system of the modern society. Its protection is an international existential concern.

References:

1. The Department of Defense Cyber Strategy, April 2015.
2. Nathalie Caplan, Cyber War: the Challenge to National Security, Global Security Studies, University of North Carolina Wilmington, Winter 2013, Volume 4, Issue 1.
3. Cyberspace Operations, Air Force Doctrine Document 3-12, 15 July 2010.
4. Kai Denker, Cyber war and Cyber crime – Implications of a Vague Difference, TU Darmstadt, Apr 8, 2011.
5. lieutenant colonel Scott W. Beidleman, Defining and Deterring Cyber War, U.S. Army War College, Carlisle Barracks, PA 17013-5050, 2009.
6. Wolfgang Röhrig, Programme Manager Cyber Defence at EDA and Wg Cdr Rob Smeaton, Cyber Defence Staff Officer at EUMS CIS Directorate Cyber security and cyber defence in the EU - opportunities, synergies and challenges, 2015.
7. http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.
8. http://www.nato.int/cps/en/natohq/topics_78170.htm.
9. http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2013_10/20131022_131022-MediaBackgrounder_Cyber_Defence_en.pdf.
10. http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf
11. http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.
12. http://www.bta.bg/en/c/DF/id/1314092.
13. Department of Defense, Defense Science Board, Task Force Report: Resilient Military Systems and the Advanced Cyber Threat, January 2013.

14. Martti Lehto, Pekka Neittaanmäki, Department of Mathematical Information Technology University of Jyväskylä, Finland, Cyber Security: Analytics, Technology and Automation, 2014.
15. Valeri Rachev, Strategic and Political Dimensions of Cyber Security - Lessons from Bulgaria, Centre for Security and Defence Management, www.IT4Sec.org/csdm.