WILL THERE EVER BE A CYBER WAR?

EVIJA ŠULTE

DOI: 10.26410/SF_2/17/12

ABSTRACT

During the NATO Warsaw Summit cyberspace was recognized as a domain of operations reaffirming the necessity and requirement for the regulation of cyberspace as a potential operational environment for network-centric operations. It is linked with the fact that cyber-attacks of diverse types are continuously increasing in numbers, thus causing a significant threat to the uninterrupted functioning of governmental and public communication and information systems, data centres, financial and banking systems, national and international networks and infrastructure. This raises the question of whether it is a new domain of warfare. The paper analyses terms "cyber warfare" and "cyber war" in the contemporary context of cyber security and the forms and effects of cyber war.

KEY WORDS

Cyber security, offensive cyber capabilities, cyber warfare.

EVIJA ŠULTE, LATVIA
evija.sulte@ baltdefcol.org
Baltic Defence College
Tartu, Estonia

Introduction

In July 2016, during the NATO Warsaw Summit, the Alliance 'recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea' (CCDCOE, 2016). This decision therefore reaffirms the necessity and requirement for regulations of cyberspace as a potential operational environment for the network-centric operations. With the accelerating speed of modern technological development along with the high demand for the connectivity of various digital systems, protection of networks and security of cyberspace have become a vulnerable and challenging realm for every nation. Furthermore, all domains of national and international system depend on digital technology, relying on network infrastructure that provides the advantage of interconnectivity, near real-time communication and exchange of information and data worldwide. However, despite numerous benefits of modern technology, the cyberspace has also enabled a new platform for the opponents to exploit and a surface to launch an attack from. Cyber-attacks of diverse types are continuously increasing in numbers, thus causing a significant threat to the uninterrupted functioning of governmental and public communication and information systems, data centres, financial and banking systems, national and international networks and infrastructure. This consequently raises the question whether the world is currently entering a new era of warfare, where the means to wage war and cause disruption and destruction are purely digital. Are all the offensive cyber activities conducted by single hackers, hacktivists or state-sponsored individuals/groups heading towards a potential large-scale confrontation between states? Offensive cyber capabilities developed by many states today build a powerful and efficient weapon for the potential use against an opponent in case of a conflict to achieve political, military and/or economic goals.

The connection of systems and networks to the Internet exposes them to public access and thus, through the Internet, to penetration, intrusion, attacks targeted at the systems themselves, the information they contain, and the processes they control and facilitate. There are scholars who contend that cyber-attacks cannot constitute an act of war as they lack criteria of an armed attack that should be instrumental, political, and violent per se (Rid, 2013). Nevertheless, this paper will claim that the cyber war will take place in the near future as a new form of warfare in the technologically developed world. Cyber war could be commenced because of its cost-effectiveness, a less lethal and destructive form, the potential to deter or prevent enemy's ability to the conventional use of military force, or as an option for creating the supplementary effect for any conventional military operation in the initial phase of an armed conflict. To support this argumentation, the first part of the paper will define the terms "cyber warfare" and "cyber war" in the contemporary context of cyber security, whereas the second part will focus on the forms and effects of cyber war.

Defining the cyber warfare and the cyber war

The recognition of cyberspace as a domain of operations encompasses the current problem that there is no consensus and united understanding reached about the definitions and terms related to the cyber domain that would explain the potential cyber operations. In particular, cyber warfare and cyber war are terms that are interchangeably used by nations and international actors without unanimously accepted definitions, and therefore are controversial in their meanings. States and international organizations have put in a great deal of effort in defining these terms, and on account of this, a wide range of definitions exist in the cyber realm. For instance, Russia and the United States have agreed on a definition that cyber warfare is to be regarded as 'cyber-attacks that are authorized by state actors against cyber infrastructure in conjunction with government campaign' (Godwin III et al., 2014, p. 43). Furthermore, RAND, the research and analysis organization Corporation suggests that the 'cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks' (RAND, 2016). Whereas the International Committee of the Red Cross defines the cyber warfare as any adverse action against an opponent intended 'to discover, alter, destroy, disrupt or transfer data stored in a computer, manipulated by a computer or transmitted through a computer' (International Committee of the Red Cross, 2010). These various definitions lead to the conclusion that the cyber warfare is any offensive cyber activity within the cyberspace that has a political background involving another state or its political actor to target the critical networks and infrastructure of the opponent country. As a result, these targeted cyber-attacks would significantly disrupt or damage the target country's ability to use the critical information and communication systems. Cyber-attacks as part of cyber warfare would therefore be referred to the instruments of national power of one state to influence another state by conveying political messages to the targeted state or causing social, financial or other economic damage without the use of physical force or employment of military force.

To distinguish the nature and scale of offensive cyber activities, the distinction between cyber warfare and cyber war has to be made. A wide variety of available definitions describes the aspects that would be related to an interstate conflict and would constitute the offensive cyber actions as cyber war. For instance, Belgium (2012) and Austria (2013) offer coherent and comprehensive definitions associating cyber war with the rapid and large-scale acts of aggression executed by one state against another one by using cyber means and conducting activities in support of conventional military operations to achieve national goals. Furthermore, the following definition is provided by Russia and the United States describing cyber war as 'an escalated state of cyber conflict between or among states in which cyber-attacks are carried out by state actors against cyber infrastructure as part of a military campaign' (Godwin III et al., 2014, p. 32). In line with these definitions, it has to be underlined that a cyber war encompasses the means to launch digital attacks, applies the use of force against opponent's critical infrastructure, networks, and information and communication systems, as well as conducts military operations in support of overall political aims to resolve the matter of conflict between states. In this context, cyber war is referred to combined political and military actions using the cyberspace as the platform to launch the attacks from against another state in order to achieve strategic political goals. This paper supports the reasoning that cyber war will be related to a form of war between states, and will be used in conjunction with other military actions and campaigns. Cyber war could therefore be considered as a form of power wielded with specific weapons and capabilities to be used to gain power, influence the international system and execute military operations.

Furthermore, it has to be emphasized that the protection of networks, systems and data is essential to the safety and security of national, public and private actors, and that offensive actions through the cyber domain against any of these actors can threaten their continuity, stability and prosperity. Well-prepared and coordinated offensive cyber operations can seriously disrupt disparate electronic systems, and infect and damage network infrastructure. Moreover, they can cause physical damage and limit access to the critical services thus paralyzing interconnected processes and functions of a state. In this context, states should have a novel approach to defining the current and future threats, risks and vulnerabilities, and carry out a realistic and comprehensive assessment of the potential outcome of any cyber related danger. For this purpose, as underlined by the United Nations Institute for Disarmament Research (2013), there are many countries (i.e. the United States, France, India, China, Russia) that have included the development of offensive cyber capabilities in their cyber security strategies. The offensive cyber capability will be referred to as 'a capability to initiate a cyber-attack that may be used as a cyber deterrent' (Godwin III et al., 2014,

p. 49). However, most countries do not state publicly the support of offensive cyber capabilities, practicing instead the term of active cyber defence. For example, CCDCOE (2017) defines active cyber defence as an anticipatory action aimed at disclosing any attempts of cyber-attacks or the actual breaches, or to identify any cyber offensive at the earliest stage by executing pre-emptive, preventive or retaliatory cyber actions against the origin of the cyber-attack. In this context, it is important to highlight that active cyber defence involves the proactive measures while defensive cyber capabilities, as defined in Russia-U.S. Bilateral on Cybersecurity (2014), foresee only the reactive or passive measures in relation to protection or repellence against cyber acts being used as cyber deterrents.

Moreover, it has to be taken into consideration that the growth and expansion of technological potential will continue to increase in the future, thus providing the capabilities to shape the future battlefield in the cyber domain. Taking these factors into account, cyber wars will not only be part of any interstate conflict in the future, they will also exist as separately planned and executed acts of war against the opponent states.

Cyber war as a less lethal and destructive form of war

In today's globalized and technologically developed world where every action is recorded, any form of violence, unnecessary suffering and collateral damage is strongly condemned by the whole society. From this perspective, a cyber war launched from any of the digital platforms would be chosen as a less destructive form of war causing less casualties than any other armed engagement. 'For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill' (Sun Tzu in Griffith, 2011). Following this logic, a cyber war would offer a potential aggressor an option of influencing its opponent without direct attacks against its force. Instead, it would allow the engagement by other, non-conventional means thus affecting its critical capabilities and not its conventional forces. As Farwell and Rohozinski (2012) note, there is no need to defeat the opponent in order to attain certain national goals, moreover cyber weapons would provide non-lethal means to disable the adversary's operational potential. Cyber weapons like digital codes and malicious software are developed within the virtual domain. From this aspect, cyber weapons do not possess the kinetic qualities and can therefore be considered as non-lethal *per se*. As Rid (2013) points out, it is to be highlighted that the digital computer codes by their nature are not able to cause harm to any biological entity for the reason being developed within the digital environment, and from the technical perspective possessing the capability to affect only digital systems. In addition, Rid (2013) remarks that any system affected by hostile actions has to be changed to a weapon system first in order to enable the power and energy for further destruction of any kind, be it material or human life. All the conventional attacks and armed conflicts use traditional means and ways to achieve the strategic and military end-states by exploiting other operational domains. Waging a digital war through the cyberspace would enable the possibility to cause damage to the opponent without kinetic means being applied, thus causing less damage or destruction. Lewis (2015) argues that the majority of cyber-strikes would not result in a devastating outcome as after conventional military attacks, they would rather deny access to networks and degrade systems, thus throwing the opponent into a turmoil.

Seen from this perspective, a cyber weapon in terms of a digital malicious code or a computer virus cannot be aimed directly at a human being as a conventional weapon system. The loss of human life as a consequence of the use of cyber weapons can therefore only be a secondary effect created by the damage of the system that has been attacked.

Furthermore, cyber weapons can be developed with the aim to target specific systems or infrastructure thus not intended to cause additional, unnecessary collateral damage to achieve the political, strategic or military objectives. In parallel with the precision ammunition, cyber weapons may be used for sophisticated targeting, aiming at definite components of a digital system. As in the case of Stuxnet, which was created in the form of a malicious computer virus aiming to affect Iran's nuclear program and caused the physical damage to nuclear centrifuges, it is reasonable to deduce that this type of cyber weapon is designed for specific cyber war actions. Professor George Lucas notes that Stuxnet 'shows that cyber war can be an effective alternative to conventional war' (Lucas, 2011, p.18). More importantly, cyber weapons and applied techniques could be conceived to launch surgically precise cyber-attacks thus being efficient and reaching proportionate effects on targets (Radziwill, 2015). Cyber weapons may therefore be used for the incapacitation of vital systems without physical destruction, by damaging or temporarily disabling electronic systems controlling, for example, water plants, power grids, transportation systems etc. Another important factor to highlight with regard to the less destructive effects of cyber weapons is the fact that the damage caused by cyber-attacks can be reversible, meaning that digital systems can be restored and brought back online easier and quicker than it takes to reconstruct and rebuild the infrastructure after any conventional use of weapons such as air strikes and bombardments. This aspect is supported by Farwell and Rohozinski (2011), who claim that cyber-strike has in this regard the advantage of reaching the ends with fewer casualties among the civilian population in comparison with air strikes. Moreover, as McGraw (2013) argues, it does not require large national and state resources to develop as effective cyber weapon as Stuxnet. Owing to the fact that the development of this sort of effective cyber war payload is less complicated and takes less effort than to develop conventional military capabilities, cyber war is for this reason cost-effective and thus also unavoidable (McGraw, 2013). In addition, evaluating the ethical side of cyber war, Arquilla (2013) notes that because of the fact that digital units like bits and bytes would disrupt rather than destroy the targeted system, a cyber war would be considered less problematic from the ethical perspective. Moreover, given the circumstances when a physical engagement does not follow, cyber war would cause practically no physical damage or loss of life. With that in mind, digital weapons could replace conventional combat weapons, save extensive amounts of national resources and require comparatively less combat personnel to apply these weapons into actions, and by all this still achieving the political goals with less cost in resources and human lives.

Cyber war as a preventive war

With the development of operational concepts that are enabled by the sophisticated technologies, cyber war as a future form of war would be launched as a preventive war to stop the enemy state from starting the war, either of a hybrid or conventional character. This type of cyber war would be used as a separate deterrent act, and it would not be linked to the conventional military operation. Lebow (2007) describes deterrence as the influential process that allows for impeding any unwanted activity by assuring the involved actor that the benefits gained could not be worth the expenses. Following this logic, the cyber war in a form of preventive war would have the effect of deterrence that would either prevent enemy from engaging in war with a threatened state or it would compel the opponent to act according to the attacker's will and request. Researchers on cyber deterrence theories like Jensen (2012) highlight that cyber deterrence is to be regarded to all the parties, be it individuals, groups or states, and it comprises the whole range of offensive cyber activities that could potentially create kinetic effects, thus achieving the desired end-state of respective party. When assessing the causes of such preventive wars and evaluating the justification of those, Lucas argues that the efforts to defuse a crisis prior a military offensive is launched would therefore justify the preventive war if other attempts of conflict resolution have failed. Moreover, he adds that the preventive cyber war would be 'focusing solely on threatening' (Lucas, 2011, p.18), and would be aimed at strategic military objectives, thus being directed against the critical and essential enemy military command and control infrastructure. With the accelerated sophistication of information and communication technologies, it would be possible to achieve a wide range of effects on the adversary by the application of various cyber-attack methods and techniques. These could vary from the disruption of critical services, denial of access to the essential infrastructure to the physical destruction of networks and interlinked systems or capabilities. On a national level most of the financial, media, communication systems are interlinked already, and there is a tendency within the military domain to achieve maximum interoperability between various information technology systems as well. The militaries around the world put in a considerable effort to interlink the systems not only internally within separate military services and components but also between the components and the higher commands. They use different digital and computerized systems like command and control information systems, weapon platforms and sensors that are linked together or interconnected with each other, as well as connected to the external networks via the Internet. Furthermore, the interoperability between various military systems is becoming more and more critical to enable faster communication, the exchange of mission essential data and provide better situational awareness and control over ongoing operations. In addition to this, Richard A. Clarke and Robert K. Knake (2011) argue that besides the fact that ever increasing number of critical systems are put online, also human-made flaws in software and hardware development and the public Internet vulnerability should be considered as the potential drivers for the opponents to exploit the opportunities of accessing essential and critical information and data. In consequence, the interconnectivity and interlinkage of military networks, digital weapon platforms and communication and information systems can become large high value targets of external influence and attacks when being online. Based on this, the preventive cyber war would therefore be effective to deny the enemy the use of most critical infrastructure for its own military purposes, thus delaying or preventing the enemy to launch an attack with the conventional means.

Cyber war as a part of conventional war

The future armed conflicts and conventional use of military force between state actors would include cyber war as part of the generally recognized warfighting function to gain the effects of initiative, surprise and momentum while confusing the targeted state of the character and nature of the cyber-attack. Italian air power strategist General Giulio Douhet notes that 'Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur' (Douhet, 1921, p.30). In this context, it is of the highest importance for any nation to comprehend the challenges associated with the development of cyber domain and the contemporary (CCDCOE, 2016) and future threats it may pose. Many countries are developing their capabilities incrementally to conduct an offensive cyber action, and many more will ultimately procure and improve these capabilities as active defence means. According to Lewis (2015), cyberstrikes are part of the current military doctrine of potential adversaries with the aim to design the early stages of conflict and delay NATO's capability to react. Offensive cyber actions in advance of any conventional use of military force would enable the potential enemy to gain advantage and surprise while the target state would not be able to react and respond immediately to the imminent conventional threat. Arquilla (2013) describes the cyber war as an exceptionally powerful and covert instrument to be utilized at the early stage of the war. Moreover, a war initiated by cyber-surprise could contribute to the victory, at the same time reducing the number of casualties, and causing less harm to the adversary, as well as own forces (Arquilla, 2013).

As James A. Lewis (2015) points out the possible target to be chosen before the actual conventional use of military force would be the so-called 'war-supporting infrastructure'. Thus referring to the most critical infrastructure, networks and systems that provide electricity and power, transportation services, access to different financial and media systems, information and communication systems and official websites of targeted state's government (Lewis, 2015). He also adds that these objects would be valuable and interesting targets for cyberstrikes as part of military campaigns. The initial cyber war activities would allow the external control over the critical networks, systems and infrastructure thus denying their use by the targeted state. One of the aims for the initial cyber war to take place would be to incapacitate the targeted state in terms of taking over the control of its surveillance and control systems thus "blinding" it for a specific period of time. In case these systems have been disabled to the extent required for the conventional attack to be launched, the attacking state would enjoy the advantage of not being seen by land, air or navy surveillance systems, and would require the targeted state to use its conventional military forces to acquire the necessary operational information. Clarke and Knake (2011) argue that modern societies and governments are excessively relying on different computer systems that enable their functioning. The current dependency on cyberspace expose each and every nation along with their military forces to the vulnerabilities coming from and through the public access to the Internet. With different systems and networks being interconnected within the military realm and beyond it, the opponent might be able to exploit this opportunity in order to take out all vital and essential systems of the target state, and even get access to the restricted networks through the gateways interconnecting the different systems. Farwell and Rohozinski (2012) emphasize that effective use of cyber weapons may disrupt the opponent's military forces to be used efficiently by reducing the speed of mobilization, assemblage and deployments thus ruining the momentum of attack. They underline that disabling adversary's critical networks and services could be a wiser approach than physical destruction of the adversary. Moreover, future cyber weapons will be targeted at enemy's capability to operate within the operational area, limit its command and control, and therefore hindering the enemy decision makers from accomplishing the mission and furthermore, from reaching operational or strategic goals (Farwell and Rohozinski, 2012). This being said, the cyber war will be the initial crucial phase for any conventional warfighting scenario providing the advantage and freedom of action to the party having the offensive incentive to strike first. Furthermore, the cyber war as a covert part of future military offensive actions will enable the initiative, momentum and surprise thus confusing and incapacitating the targeted state, and will therefore, without doubt, be a part of every military operation or campaign in the future.

Conclusion

In conclusion, it has to be reemphasized that the latest decision of NATO to recognize the cyber domain as a potential operational domain reassures the crucial role of cyber realm in the contemporary global security arena. With the sophistication of technology and increased development of cyber capabilities, both defensive but especially offensive ones, the cyber domain becomes a potential future battlefield for countries to achieve their political, strategic, military or economic goals. The proliferation of cyber weapons constitutes a threat that might be directed against opponent country to wage cyber war in order to influence the targeted state's decisions or actions. In this context, cyber war creates the possibility to engage the targeted state with less resources than a conventional military action would require, therefore cyber war as a form of war is highly possible, if not inevitable. Reconsidering the possibilities and the goals of countries to launch a cyber war, and reassessing the current trends of recent and ongoing armed conflicts, the future cyber war could be associated with either a preventive type of action or as a part of a conventional war. The former type of cyber war would be aimed at stopping the enemy state from starting the war, therefore having either coercive or deterrent effect. Whereas the latter form of war would be waged in order to achieve the moment of surprise and at the same time degrading enemy state's capabilities to accordingly react and respond to the conventional military engagement. The cyber war in either form would carry the potential of disabling targeted state's critical infrastructure, command and control information systems, governmental and military networks. This would constrain its ability to coordinate actions and efforts, organize forces and operate within the battlespace be it only within the cyberspace or in other operational domains. In comparison with the conventional armed conflicts and the use of military force, and being embodied within the cyber domain, cyber weapons and cyber war carry no lethal energy per se. From this perspective, cyber war would be considered as a less lethal and less destructive war, causing less human casualties and collateral damage than any form of conventional use of arms and weapons. Taking all the aspects into consideration, it has to be noted that the reasons and causes of wars will be mainly the same, be it political, economic or social, however, the forms and ways to wage wars will continue to change in the future. With the ever-evolving technologies, development of sophisticated cyber capabilities makes one to assume that cyber war is inevitable in case of potential confrontation between states. Nowadays, living in an era of pervasive digitisation and with many vital and critical systems being online and interconnected, it is almost impossible to avoid the dependency on cyberspace. Nevertheless, in anticipation of potential threats, nations should build resilient and robust cyber capabilities and envisage alternatives in case of cyber-attacks against the most vulnerable and critical infrastructure, systems and networks. In addition, states should change their pure defensive cyber posture towards a more proactive one in order to detect hostile cyber activity and be prepared to launch a counter-operation to prevent the further damage, deny or destruction of the systems the country is the most dependent. Only by planning preventive measures, the effects caused by potential cyber war would be less destructive and paralyzing.

References

Arquilla, J., 2013, Twenty years of Cyberwar. Journal of Military Ethics, 12(1), pp. 80-87.

Austria, 2013, Austrian Cyber Security Strategy. [online] Vienna: Federal Chancellery of the Republic of Austria. Available at: https://www.bka.gv.at/DocView.axd?CobId=50999 (accessed 26 Nov. 2016).

Belgium, 2012, Cyber Security Strategy. Securing Cyberspace. [online] Available at: https://www.b-ccentre.be/wp-content/uploads/2013/03/cybersecustra_nl.pdf (accessed 26 Nov. 2016).

CCDCOE, 2016, NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit, [online] Available at: https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html (accessed 10 OCT 2016).

CCDCOE, 2017, Cyber Definitions. [online] CCDCOE. Available at: https://ccdcoe.org/cyber-definitions.html (accessed 26 Nov. 2016).

Douhet, G., 1942, The command of the air. New York: Arno Press Inc., N.Y.

Farwell, J., Rohozinski, R., 2011, Stuxnet and the Future of Cyber War. Survival, 53(1), pp. 23-40.

Farwell, J., Rohozinski, R., 2012, The New Reality of Cyber War. Survival, 54(4), pp. 107-120.

Godwin III, J., Kulpin, A., Rauscher, K. and Yaschenko, V., 2014, The Russia-U.S. on Cybersecurity – Critical Terminology Foundations 2. 2nd ed. [online] EastWest Institute and the Information Security Institute of Moscow State University, pp. 32, 43. Available at: https://www.files.ethz.ch/isn/178418/terminology2.pdf (accessed 26 Nov. 2016).

International Committee of the Red Cross, 2010, Cyber warfare. [online] Available at: https://www.icrc.org/en/document/cyber-warfare (accessed 20 Mar. 2017).

Jensen, E.T., 2012, Cyber deterrence. Emory International Law Review Vol. 26 (2), pp. 773-824

Knake, R., Clarke, R., 2011, Cyber war: The next threat to national security and what to do about it. New York: HarperCollins Publishers.

Lebow, R., 2007, Coercion, cooperation, and ethics in international relations. New York: Taylor & Francis.

Lewis, J.A., 2015, The role of offensive cyber operations in NATO's Collective defence. Tallinn Paper No. 8, Tallinn Papers, NATO Cooperative Cyber Defence Centre of Excellence

LUCAS, G., 2014, Permissible Preventive Cyberwar: Restricting Cyber Conflict to Justified Military Targets. In: L. Floridi and M. Taddeo, ed., The Ethics of Information Warfare, Springer International Publishing AG, p. 81.

Mcgraw, G., 2013, Cyber War is Inevitable (Unless We Build Security In). Journal of Strategic Studies, 36(1), pp. 109-119.

Radziwill, Y., 2015, Cyber-attacks and the exploitable imperfection of international law. Leiden: Brill Nijhoff.

Rand, 2016, Cyber Warfare. [online] Available at: http://www.rand.org/topics/cyber-warfare.html (accessed 12 Nov. 2016).

Rid, T., 2013, More attacks, less violence. Journal of Strategic Studies Vol. 36 (1), pp. 139-142.

Sun Tzu, Griffith, S., 2011, The art of war. 1st ed. London: Watkins Publishing.

UNIDIR, 2013, The Cyber Index. International Security Trends and Realities. UNIDIR/2013/3. [online] New York, Geneva: United Nations Institute for Disarmament Research. Available at: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf (accessed 26 Nov. 2016).