ISSN: 2630-6166
Journal IKSAD

JOURNAL OF INSTITUTE OF ECONOMIC DEVELOPMENT AND SOCIAL RESEARCHES

ISSN: 2630-6166

International Refeered & Indexed 2018 Open Access Refeered E-Journal
Vol:4 / Issue:9 iksadjournal.com / iksadjournal@gmail.com p.195-214
Article Arrival Date 28/03/2018 JUNE 2018 Published Date 26.06.2018

RETHINKING CYBER WARFARE: TIMELESS, NORMLESS AND UNCONSTRAINED

SİBER SAVAŞI YENİDEN DÜŞÜNMEK: ZAMANSIZ, KURALSIZ VE SINIRSIZ

Pınar AKARÇAY

Dr., Visiting Researcher, Institute for Housing and Urban Research, Uppsala University, Uppsala, Sweden

Gökhan AK

Dr., Faculty of Economics, Administrative and Social Sciences, Nişantaşı University, İstanbul, Turkey

ABSTRACT

Improvements in cybernetics have made likely far reaching shifts in all areas of life. Thus, the scientific-technological developments after 1950s gave rise to "the information revolution" from which national security has quite been affected as well. The rapid growth in the fields of computing created a new realm of fantasy called cyberspace. As a phenomenon, cyberspace has the potential for enormous avails and advantages as well as unpredictable risks. There are three major dimensions all associated with cyberspace: technologies, policies and disputes. In order to analyze the real damage that a hypothetical cyber-war or individual act of cyber warfare could do to the citizens of any nation coming under attack, it is fundamental to begin with some reflections which will help us reach a full understanding of the phenomenon, and its related practical implications as well as impacts. Since cyberspace comprises many complicating matters, it is a further difficulty of developing new combative techniques, tools and norms in an area that is inherently secretive. Cyber-attackers do not announce who they are and the victims may not want to admit having been vulnerable. By this view, this research will specifically examine timeless, normless and unconstrained cyber warfare by rethinking its history, content, associated emerging policies and focus on the question of national security in light of the cyberspace phenomenon.

Key words: Cyberspace, Cybernetics, Cyber Warfare, Cyber-Attack, National Security.

ÖZET

Sibernetikteki gelişmeler, yaşamın her alanında uzun erişimli değişiklikler meydana getirmiştir. Böylece, 1950'lerden sonraki bilimsel-teknolojik ilerlemeler, ulusal güvenliğin de kendisinden oldukça etkilendiği, "bilgi devrimi"ne yol açmıştır. Bilgi-işlem alanındaki hızlı gelişme, siber alem olarak bilinen yeni bir fantastik dünya yaratmıştır. Bir fenomen olarak siber alem, büyük imkan ve avantajlarının yanında bilinmedik riskleri de içerisinde barındırma potansiyeline sahiptir. Hepsi siber alem ile ilgili olmak üzere üç ana kısım mevcuttur: teknolojiler, siyasalar ve anlaşmazlıklar. Sanal bir siber savaş veya herhangi bir ülkenin vatandaşlarına karşı girişilebilecek bireysel bir siber saldırının yapabileceği gerçek hasarın analizi için, bu fenomeni tam olarak anlayabilmemize yardımcı olabilecek türden bazı etkileri analiz, bunun Pratik sonuçları ile başlamak temel bir gerekliliktir. Siber alem birbiriyle çelişkili bir çok konu içerdiğinden, aslında tamemen gizli bir alanda yeni savaşma normları, araçları ve teknikleri üretmek oldukça zor bir konudur. Siber saldıranlar, kendilerinin kim olduğunu belirtmez ve kurbanlar da kendilerinin saldırılara açık olduğunu kabule pek yanaşmazlar. Bu çerçevede, bu çalışma özellikle zamansız, kuralsız ve sınırsız özelliklere sahip siber savaşı, siber alem fenomeni bağlamında, tarihsel, içerik, ilgili yeni gelişen siyasalar ve ulusal güvenlik sorunuyla olan ilişkisine odaklanarak inceleyecektir.

Anahtar Kelimeler: Siber Dünya, Sibernetik, Siber Savaş, Siber Saldırı, Ulusal Güvenlik.

"*An invasion of armies can be resisted; an invasion of ideas cannot be resisted.*"[1]

1. INTRODUCTION

It is cyberspace and war in it about which we should seriously concern. The reason behind that presumes a bright past, but a likely-dark future regarding cyberspace, information technologies, and cybernetics. Accordingly, developments in computers have made probable far reaching shifts in all areas of our lives, and the rapid progress in computing, communications, and software. Since the

[1] Victor Hugo, ***The History of a Crime***, T.H. Joyce and Arthur Locker (trans.), Nabu Press, Charleston, SC, 2010, p. 415.

1950s and the launch of the first satellite in 1957, there has been competition between the superpowers over the means of reaching and staying in space, and over nearby planets. Progress in this domain gained momentum as a result of the appearance of computing and electronics.[2] These speedy improvements in the spheres of computing and communications have gave pace to a rapidly-changing domain which is also unbelievably thriving beyond predicts. This phenomenal sphere is cyberspace. It is a domain created not in nature but by human beings. This space has also created its own potential for huge benefits; but unfortunately for timeless, normless and unconstrained threats; that is to say, risks from an unpredictable, unknown and unreliable space. That is why, while existing effectively nearly for fifty years at most, we are in great trouble in understanding of this phenomenon; because it is just beginning. By this view, we could describe cyberspace as a new phenomenon.[3] Threats of today's cyberspace, which were inherited from 20th century humane and innocent cybernetics improvements have naturally posed great risks for the national security since terrorism of all kinds and in all domains are the greatest enemy of mankind. Thus, societies as well as nations and states are more vulnerable today to an unknown risk roaming like a ghost in the cyberspace.

"Cyber warfare" is becoming a much-used term, albeit with very little agreement as to its precise meaning. Some see cyber warfare (or even full-scale, self-contained cyber-war) as the new paradigm for inter-state conflict. Others see it as little more than a string of alarmist anecdotes, which often seem closer to the world of science fiction than public policy. The median position is to suggest that cyber warfare is at least becoming one aspect of inter-state conflict with several distinguishing features. In some cases, the parallels with conventional and economic warfare are clear. But in other respects cyber warfare would require new thinking and new practice where conflict between states is concerned.[4]

By hitting road from these factual aspects, we could emphasize again that impressing estimation that cyberspace and war in it should seriously be concerned nowadays, particularly in the context of national security. The reason behind that puts forth a crystal-clear stand that national security has quite been affected by the information revolution and the cyberspace phenomenon. Smart use of a new sphere like cyberspace allowed previously unknown capabilities, which together with new methods have generated a qualitative change in the military field.[5] However, a public discussion on the issue of cyber security, as of other new hi-tech fields, is lacking in many states[6] as happening in, for instance, Turkey as well at present times. Since cyberspace comprises many complicating matters, it is a further difficulty of developing new combative techniques, tools and norms in an area that is inherently secretive. It is virtually impossible to identify every cyber-attack that occurs. Some can operate undetected for years. Others are brief, but still leave no detectable trace. Thus, cyber-attackers do not announce who they are and the victims may not want to admit having been vulnerable. By this view, this essay will specifically examine cyber warfare by rethinking its historical context, technological content, associated emerging policies. Thus, this research will focus on the question of cyber warfare and related security in light of the cyberspace phenomenon, while aiming to survey the field and create a common language for a fruitful public discussion of the developing issue of cyber warfare related security. This discussion paper will also be concerned with states and societies (rather than businesses or individuals) and their vulnerability, through interconnectedness and dependence, to aggressive warfare action either from, or facilitated by cyberspace. Because cyber warfare should indeed be considered a strategic problem, if we may so claim.[7]

---

[2] Lior Tabansky, "Basic Concepts in Cyber Warfare", *Military and Strategic Affairs*, Vol. 3, No. 1, May 2011, p. 89.
[3] Isaac Ben-Israel, "From the Sword's Blade to Computer Memory", *Odyssey*, No. 9, October 2010, p. 5.
[4] Paul Cornish, "The Vulnerabilities of Developed States to Economic Cyber Warfare", *Chatham House Working Paper*, London, June 2011, p. 6.
[5] For a discussion of the information technology revolution in military affairs, see Michael E. O'Hanlon, *Technological Change and the Future of Warfare*, Brookings Institution Press, Washington, D.C., 2000; Stuart E. Johnson, and Martin C. Libicki, , *Dominant Battlespace Knowledge: The Winning Edge*, National Defense University Press, Washington, D.C., 1995; Isaac Ben-Israel, "Security, Technology, and the Future Battlefield," in Haggai Golan, ed., *The Texture of Security*, Maarachot, Tel Aviv, 2001, pp. 269-327.
[6] Tabansky, "Basic Concepts in Cyber Warfare", pp. 75-76.
[7] HM (Her Majesty) Government, "A Strong Britain in an Age of Uncertainty: The National Security Strategy", TSO, Cm 7953, October 2010, London, p.10. Available at: http://www.official-documents.gov.uk/ (Visited on 22 January 2018) In the words of the 2010 UK National Security Strategy, national strategy must be "*...a combination of ends (what we are seeking to achieve), ways (the ways by which we seek to achieve those ends) and means (the resources we can devote to achieving the ends).*"

2. ASSESSING CYBERSPACE VS. CYBER WARFARE: HISTORICAL FUNDAMENTALS AND PROPERTIES

Let's commence by asking what the cyber warfare is. Unlike nuclear explosion where millions would die the disruption created within a society or for a group by a major cyber-attack or war may be just as serious. As Cetron and Davies observe; "*…major concern is no longer weapons of mass destruction, but weapons of mass disruption.*"[8] Thus, a small sample of definitions is provided to give a taste of the approaches and ideas that have been articulated; "*The Shanghai Cooperation Organization has defined "information war" in part as a "confrontation between two or more states in the information space aimed at… undermining political, economic, and social systems [or] mass psychologic [sic] brainwashing to destabilize society and state.*"[9] For Nye, "*Cyber power is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain.*"[10] The literature and occurrences in the system show that non-state actors are significantly involved in conducting cyber war.[11] The reason for the inclusion of more actors within this emerging realm is that information and the use of information is growing across the globe. But as the use of information grows there is also an increased threat to the control of civilization.[12]

The central features of the 'cybered' world of the early 21st century are the interconnectedness of global communications, information and economic infrastructures and the dependence upon those infrastructures in order to govern, to do business or simply to live. The more fundamental observation is that developed societies seem unwilling or unable to take counsel of their fears about cyber space. Perhaps because the world is so interconnected, and perhaps because societies depend so much on the complex of infrastructures for what is needed and desired, there is a reluctance to accept, and in some quarters an inability to understand that these highly developed societies have made themselves vulnerable to miscreants, criminals and aggressors. Technological strength and superiority has, unfairly though it might seem to its originators and beneficiaries, prompted what military analysts would describe as 'asymmetric' vulnerability, where a fleet-footed and sharp-witted adversary can maneuver so fast and so decisively that the strongest and most elaborate defenses are turned into a cumbersome liability and a disadvantage.

If one were to apply only the strategy of defense in the realm of cyber war, this choice is defective from the start. Defending computers and networks has created a massive sector which develops and maintains security; the capacity of this approach is always being threatened. First and foremost the defensive aspects of cyber war are at a disadvantage due to the 'offensive dominance' which has been shown to this point. [13] Second, these defenses are never going to be perfect either due to programming issues, the need for the system to be connected to the larger internet, or human error. The only way to completely protect a system from external threats would be to full segregate the system from external connection, but even by doing this the system still could be threatened by the human element either intentional or not.[14] There are arguments that governments are required to help defend private networks and sites due to inter-connectiveness.[15] Since too little is known about who might wish to use cyber space against developed societies, and to what end, it is at least notionally possible that developed societies might be comprehensively, structurally vulnerable to a well-organized and

[8] Marvin J. Cetron and Owen Davies, "Ten Critical Trends for Cyber Security", *The Futurist*, Vol. 43, No. 5, 2009, p. 47.
[9] Tom Gjelten, "Shadow Wars: Debating Cyber Disarmament", *World Affairs*, Vol. 173, No. 4, November/December 2010, pp. 36.
[10] Joseph S. Nye, *Cyber Power*, Harvard Kennedy School, Cambridge, MA, 2010, pp. 3-4.
[11] See Alexander Klimburg, "Mobilising Cyber Power", *Survival*, Vol. 53, No. 1, 2011, pp. 41-60; George Patterson Manson, III,, "Cyberwar: The United States and China Prepare for the Next Generation of Conflict", *Comparative Strategy*, Vol. 30, No. 2, 2011, pp. 121-133.
[12] Lionel D. Alford, "Cyber Warfare: A New Doctrine and Taxonomy", *Crosstalk: Journal of Defense Software Engineering*, Vol. 14, No. 4, 2001, p. 28.
[13] Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, "On Cyber War", *Chatham House Working Paper*, London, 2010. Available at: http://www.chathamhouse.org/ publications/papers/view/109508 (Visited on 28 December 2017)
[14] Hans Brechbühl, Robert Bruce, Scott Dynes and M. Eric Johnson, "Protecting Critical Information Infrastructure: Developing Cybersecurity Policy", *Information Technology for Development*, Vol. 16, No. 1, 2010, pp. 83-91.
[15] Eric Talbot Jensen, "Cyber Warfare and Precautions Against the Effects of Attacks", *Texas Law Review*, No. 88, 2010, pp. 1533-1569.

capable cyber aggressor of some sort, able to turn a society's dependencies into vulnerabilities and strengths into weaknesses.[16]

Cyber-war is insidious, invisible to most, and is fought out of sight. It takes place in cyberspace, a location that cannot be seen, touched, nor felt. Cyberspace has been defined as the fifth domain of war.[17] Thus, cyberspace is arguably best understood as the 'fifth battlespace', alongside the more traditional arenas of land, sea, air and space. By this view, cyber warfare is a new but not entirely separate component of the multifaceted environment in which modern conflict takes place. Cyber warfare also holds out the possibility of achieving political and strategic goals without the need for armed conflict, by making it possible to attack the machinery of state, financial institutions, the national energy and transport infrastructure and public morale.[18]

The term "cyberspace" -cyber(netics) + space- appeared for the first time in science fiction.[19] The word comes from the Greek *kybernetes*, which means one who steers or governs,[20] and its modern form appeared in a 1948 book by mathematician Norbert Wiener to describe the study of command and control and communications in the animal world or the mechanical world.[21] "Space" has many meanings in English, referring to philosophical, physical, mathematical, geographical, social, psychological, and other properties. One definition of space is "*a boundless, three-dimensional extent in which objects and events occur and have relative position and direction.*"[22] This simple definition is sufficient for most of the daily experience of human beings, but it is not sufficient for the computerized world, which is inherently different from physical space. Thus, use of the word "space" without precise delimitation is apt to lead to conceptual difficulties, as indeed occurs with "cyberspace."[23] By this view, we could determine that cyberspace was formed by connecting computerized networks that communicate among themselves. Thus, cyberspace can be described as composed of three layers.[24] The most concrete layer, the infrastructure of the cyber world, is the physical layer. The second layer is software logic. Most of cyberspace today uses standard hardware and software, like mostly known as Internet.[25] Internet seems easy to be controlled.[26] The third layer of cyberspace is the layer of data that the machine contains and that creates information. This is the least concrete layer of the three, mainly because information properties are very different from the properties of physical objects.

Regarding disguised goals of cyber threat and cyber terrorism, it could also be in the economic interests of the predator to preserve and exploit, rather than attack and destroy the target economy and its cyber infrastructure. This might indicate that only highly committed, adversarial non-state actors (such as terrorist organizations) would wish to use cyberspace in order to inflict severe economic disruption on a developed state, on the grounds that the organization carrying out the attack would have little or nothing to lose economically in the process. Yet so far terrorist groups have been more interested in cyberspace as a means to fund their core activities rather than as a preferred medium of attack. It is certainly the case, as Nye puts it, that "*…the barriers to entry in the cyber domain are so low that non-state actors and small states can play significant roles at low levels of cost.*"[27]

---

[16] Cornish, "The Vulnerabilities of Developed States to Economic Cyber Warfare", p. 2.
[17] Fred Schreier, "On Cyberwarfare", *DCAF Horizon 2015 Working Paper No. 7*, The Geneva Centre for the Democratic Control of Armed Forces (DCAF), Geneva, 2013, p. 5.
[18] Ibid., p. 6.
[19] Andrew M. Colman, *A Dictionary of Psychology*, Oxford University Press, Oxford, UK, 2009, p. 44.
[20] Julia Cresswell, *Oxford Dictionary of Word Origins*, "cybernetics." Oxford Reference Online, Oxford University Press, Oxford, UK, http://www.oxfordreference.com/views/ENTRY.html? subview=Main&entry=t292.e1374 (Visited on 06 January 2018)
[21] Norbert Wiener, *Cybernetics or Control and Communication in the Animal and the Machine*, John Wiley and Sons, New York, 1955.
[22] *Encyclopædia Britannica*, 2010, "space," Encyclopædia Britannica Online, http:// www.britannica.com/EBchecked/topic/557313/space (Visited on 06 January 2018)
[23] Tabansky, "Basic Concepts in Cyber Warfare", p. 76.
[24] Martin C. Libicki, "Cyberdeterrence and Cyberwar", RAND Corporation, Santa Monica, 2009. Available at: http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf. (Visited on 21 January 2018)
[25] Lawrence Lessig, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.
[26] However, the reality is more complicated. For a discussion of the control structure of the internet, see Jack L. Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World*, Oxford University Press, New York, 2006.
[27] Joseph S. Nye, *Cyber Power*, Harvard Kennedy School (Belfer Center), Cambridge, MA, 2010, p. 4.

We could at this point indicate strongly that cyber warfare poses significant challenges to national securities and economies.[28] This is a crystal-clear fact also for super powers like USA or Russian Federation. For instance, former US Secretary of Defense Leon Panetta once described cyber warfare as "*…the most serious threat in the twenty-first century*", capable of destroying our entire infrastructure and crippling the nation. As one response to these challenges, the United States issued an *International Strategy for Cyberspace* in May 2011.[29] In the very first beginning of this strategy work, "*This world—cyberspace—is a world that we depend on every single day... [it] has made us more interconnected than at any time in human history.*" was stated by former U.S. President Barak Obama by emphasizing the need to deal with cyber threats seriously.[30] One pillar of this strategy recognizes the "borderless" international dimension of cyberspace and identifies the need to achieve stability and address cyber threats through the development of international norms.[31]

So, what are international norms? This question needs to be answered and provided a theoretical underpinning for how norms emerge, spread, and ultimately impact state behavior. First, norms should be introduced, with a discussion of how they are considered in the context of various international relations theories such as mainly norm evolution theory -grounded in extensive literature from fields such as international relations, sociology, economics, evolutionary biology, organizational theory, and other disciplines- will provide the foundation for later future discussions of norms regarding emerging-technology weapons, such as chemical and biological weapons, strategic bombing, nuclear weapons, and, of course, cyber warfare.[32] One category of ideas is known as norms, which are shared expectations of appropriate behavior. Norms exist at various levels and apply to different actors. In the international arena, these nonbinding shared expectations can, to some degree, constrain and regulate the behavior of international actors and, in that sense, have a structural impact on the international system as a whole.[33]

Then we may ask at this point what limits the law of war imposes on cyber-attacks. Does cyber warfare have limits and rules? Are civilian computers, networks and cyber infrastructure protected against cyber-attacks? A group of international legal and military experts says "yes" regarding these questions in the Tallinn Manual.[34] This manual is an important step towards underscoring the relevance of international humanitarian law (IHL) in armed conflicts of every kind, with the aim of reducing human suffering. The Tallinn Manual offers interesting perspectives in this respect. For example, it upholds the classical dichotomy between international and non-international armed conflicts, and recognizes that cyber operations alone may constitute armed conflicts depending on the circumstances – notably on the destructive effects of such operations. In this regard, the manual

[28] Nationally-based icons of international business might suffer particularly badly as a result of the flight of confidence, as alternative markets begin to appear more stable and therefore more attractive. And in the resulting turbulence, as national economic 'soft power' is undermined, so it will become ever more difficult to sustain investment in the 'hard power' of a costly and, in economic terms, non-productive national defence posture, as the current situation in many developed markets illustrates. See for detail Paul Cornish and Andrew Dorman, "Dr. Fox and the Philosopher's Stone: The Alchemy of National Defence in the Age of Austerity", *International Affairs*, Vol. 87, No. 2, March 2011, pp. 335-353.

[29] United States Presidency, "International Strategy for Cyberspace", May 2011, pp. 1-30. Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Visited on 29 January 2018)

[30] Critical infrastructures are physical or virtual systems and assets that are so crucial to a nation that any harm done to them will have a drastic effect on security, national economic security, national public health, or safety. See Barak Obama, "Executive Order 13636: Improving Critical Infrastructure Cybersecurity", *Federal Register*, Vol. 78, No. 33, Part III, Feb. 19, 2013.

[31] See for detail, Jens David Ohlin, Kevin Govern and Claire Finkelstein, *Cyberwar: Law and Ethics for Virtual Conflicts*, Oxford University Press, Oxford, UK, 2015.

[32] Ian Prasad Philbrick (Ed), "International Engagement on Cyber VI: Forum: The Role of Strategy in Securing a Nation in the Cyber Domain", *Georgetown Journal of International Affairs*, Vol. 17, No. 3, Fall/Winter 2016, pp. 1-109. The authors in this sixth special cyber issue bring a global view of some of the most troublesome aspects of cyber security that the international community faces. The Forum articles focus on the role of governments in formulating strategy to ensure the resiliency of the nation in the face of cyber-attacks. The authors provide diverse perspectives on how states can ensure resilience from cyber-attacks while balancing the constraints inherent in domestic regimes.

[33] Brian M. Mazanec, *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*, Potomac Books, Lincoln, Nebraska, 2015, pp. 3-6.

[34] Michael N. Schmitt (Ed.), *Tallinn Manual on The International Law Applicable to Cyberwarfare*, Cambridge University Press, Cambridge, U.K., 2013. Manual was developed at the request of the North Atlantic Treaty Organization (NATO) and the Cooperative Cyber Defense Center of Excellence (CCD-COE). The difficulty is that nation-states and non-state actors do not always follow laws when it comes to war. See Adam Roberts and Richard Guelff, *Documents on the Laws of War*, 3rd Ed., Oxford University Press, Oxford, 2000.

defines a "cyber-attack" under IHL as "a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.[35]

What does international law say for cyber weapons? Assessing the legality of new weapons is in the interest of all states, as it will help them ensure that their armed forces act in accordance with their international obligations. Article 36 of the 1977 Protocol I additional to the Geneva Conventions[36] requires each state party to make sure that any new weapons it deploys or considers deploying comply with the rules of IHL, another point usefully recalled by the Tallinn Manual. At the 28th International Conference of the Red Cross and Red Crescent, in 2003, states party to the Geneva Conventions called for "rigorous and multidisciplinary review" of new weapons and means and methods of warfare, to make sure that the law's protection is not overtaken by the development of technology. The use of cyber operations in armed conflict is a perfect example of such rapid technological development.[37]

3. MAPPING CYBER THREAT: FROM VIRTUAL CONFLICT To REAL DAMAGE

In order to analyze the real damage that a hypothetical cyber-war or individual act of cyber warfare could do to the citizens of any nation coming under attack, it is fundamental to begin with some reflections which will help us reach a full understanding of the phenomenon, and its related practical implications. The first of these is surely linked to the difficulty faced in defining the difference (which in the realm of cyber-space can be very subtle) between common criminals committing IT crime and so called 'cyber warriors'.[38] Beyond the commonly understood ease with which it is possible to remain completely anonymous in a conflict which, in its nature, is sometimes fought in a temporal arc of just tens of minutes, the problem of attributing responsibility for the attack does not just stem from the technical-structural elements of the web, and the material impossibility of putting a 'face' on its author, but also from the impossibility of pinpointing the precise geographical location of the attacker.[39] It is also useful to point out, even as a brief mention, that in the overwhelming majority of cases of penetration and, even more so, manipulation of critical electronic national security systems, these are carried out (and will always be carried out) under the utmost secrecy.[40]

An additional concern of this study will be given to the consideration that the weakest link in electronic security systems has always been – and will be for a long time to come – "man himself". And this is true both in terms of purely malicious, or intentional acts, and also in terms of unintentional failures. In fact, as far any system can really be said to be 'fully protected' from external attack, it is certainly possible – if not highly likely – that disloyal employees may manipulate the network and its security systems from within, installing malware and/or modifying its security settings, thereby facilitating outside access.[41]

Upon these reflections thus far on the genuine possibility of the break-out of cyber-war, we should emphasize that it is logical to deduce that cyber-war is much more likely, and perhaps more convenient, than is currently predicted. A cyber-war, in fact, would even allow smaller States, which are normally incapable of competing either militarily or economically with larger international powers, to attack the critical systems of other state targets thanks to its excellent 'cost-benefit' ratio. In fact, by exploiting technical skills and know-how which in 90% of cases are available for no cost directly on the internet, and by exploiting the actually poor level of defense capabilities seen on this 'battleground' in all those nations, which are excessively dependent on technological systems, it is

[35] International Committee of the Red Cross (ICRC), "Cyber Warfare and International Humanitarian Law: The ICRC's Position", *ICRC Food-for-Thought Paper*, June 2013, pp. 1-2; International Committee of the Red Cross (ICRC), "What Limits Does the Law of War Impose on Cyber Attacks?", 2013. Available at: https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm (Visited on 11 January 2018)
[36] Additional Protocol 1 (1977) to the Geneva Conventions 1949.
[37] ICRC, "Cyber Warfare and International Humanitarian Law…", p. 4.
[38] Stefano Mele, "Cyber Warfare and Its Damaging Effects on Citizens", September 2010, p. 5. Available at: http://stefanomele.it/public/documenti/185DOC-937.pdf. (Visited on 11 January 2018)
[39] Dancho Danchev, "Seven myths about zero day vulnerabilities debunked", 3 August 2010. Available at: http://www.zdnet.com/blog/security/seven-myths-about-zero-day-vulnerabilitiesdebunked/7026?tag=mantle_skin%3Bcontent (Visited on 18 January 2018)
[40] Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies", *The Wall Street Journal*, 8 April 2009. Available at: http://online.wsj.com/article/SB123914805204099085.html (Visited on 05 January 2018)
[41] Mele, "Cyber Warfare and Its Damaging Effects on Citizens", p. 7.

possible to bring this war to any part of the world, at low cost, and with a very high probability of obtaining a successful outcome. It should also be highlighted that nations with a low level of IT development, for this very reason, retain at the same time a relative strength, and an insuperable defense strategy, with regards to any possible technological counter-attack which might be carried out by 'highly digitalized' nations, meaning they possess a kind of 'general deterrent' should acts of cyber warfare be used, or should a real cyber-war break out.[42]

What has been said so far should lead to serious (and urgent) consideration being given not just to the general aspects of cyber-war and its related strategies of attack, defense and the mitigation of damage, but above all to the precise identification of what the primary targets within our national territory which can be attacked via the internet might be, even in the case of individual acts of cyber warfare. If we wish to refer only to targets where an attack could lead to the "loss of human lives", we must highlight: (1) electronic airport, civil and military air traffic and airspace control systems; (2) electronic control systems on civil and military aircraft; (3) the electronic systems of companies which design and develop the hardware and software used in airports, in air traffic control and in the construction of aircraft, both civil and military; (4) electronic national defence systems; (5) fully-automated subway control systems; (6) water supply and control systems; (7) hospital electronic systems; (8) electronic emergency management systems; (9) electricity grid management systems; (10) railway electronic systems; (11) financial and banking systems.[43] The UK defines nine national infrastructure sectors which provide these essential services: Communications, Emergency Services, Energy, Finance, Food, Government, Health, Transport, and Water.[44]

Shortly and specifically, cyber-attacks are referring to agriculture, food, water, public health, emergency services, government, defense, industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industries, and postal and shipping systems.[45] Moura found that certain types of attacks were more likely to originate from certain nations or regions. For instance, 75% of the Internet Service Providers (ISPs) containing the most phishing scams are located in the United States. Ordinary spam primarily originates in India and Vietnam, while the largest concentration of spammers per Internet address is in Nigeria. Moura also argues that analyzing where malicious hosts are concentrated could enhance prediction of future attacks. So we can emphasize that several technological methods are used to launch attacks in cyberspace.[46] However, attacks against Information Technology (IT) systems, that is to say Information Wars (IW),[47] are common and attackers are often making headlines by compromising secure and critical systems to carry out malicious activities.[48] IT systems are increasingly networked to take competitive advantage in information age, in an effort to provide better customer facilities i.e. E-commerce, instant access to information, etc. Networking of critical systems exposes them to a large pool of attackers who exploit vulnerabilities in non-secure systems – severely effecting normal business processes with malicious activities.[49]

---

[42] Ibid., p. 8.

[43] For a detailed overview of vulnerabilities relating to the management and control systems of critical infrastructure, see Idaho National Laboratory, "NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses", May 2010. Available at: http://www.fas.org/sgp/eprint/nstb.pdf (Visited on 02 February 2018); Jason Stamp, John Dillinger, William Young and Jennifer Depoy, "Common vulnerabilities in critical infrastructure control systems", November 2003. Available at: http://www.sandia.gov/ccss/documents/031172C.pdf (Visited on 14 January 2018)

[44] UK Cabinet Office, "Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards", 2009. Available at: www.cabinet office.gov.uk/media/349103/strategic-framework.pdf (Visited on 18 January 2018); UK Office of Cyber Security, "Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space", *Parliament Command Paper 7642*, London, 2009.

[45] Douglas Warfield, "Critical Infrastructures: IT Security and Threats from Private Sector Ownership", *Information Security Journal: A Global Perspective*, Vol. 21, No. 3, 2012, pp. 127-136.

[46] G. Moreira Moura, "Internet Bad Neighborhoods", *Published Doctorate Dissertation*, University of Twente, Overijssel, The Netherlands, 2013.

[47] Blank puts forth a compelling argument that deterrence in information war may not be effective given the nature of the "weapons" at work. See for detail, Stephen Blank, "Can Information Warfare Be Deterred?", *Defense Analysis*, Vol. 17, No. 2, 2001, pp. 121-138.

[48] For an in-depth discussion on relation between cyber- and net-wars, see F. Duarte Carvalho and E. Mateus Da Silva, *Cyberwar-Netwar: Security in the Information Age*, IOS Press, Amsterdam, 2006.

[49] Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, New York, N.Y., 2014, pp. 4-6.

Enterprise systems in large corporations and governments have seen less dramatic change than in personal computing, but many trends from earlier periods have continued. Older equipment has been replaced by cheaper, faster, more ubiquitous hardware and software. Organizations have become much more dependent on their technology infrastructures. Two developments in particular are worth considering: just-in-time service provision and Supervisory Control and Data Acquisition Systems (SCADA) systems.[50] The efficient provision of utility services such as electricity, gas, water and oil requires constant monitoring of supply systems. Since the 1960s these systems have been increasingly monitored and controlled using SCADA computing equipment. More recent systems incorporate load forecasting, adjusting the state of a supply network ahead of actual demand. Earlier SCADA systems were proprietary to specific vendors, but are now moving to an open networked model. Newer SCADA devices communicate using Internet protocols, sometimes over the public Internet to remove the cost of dedicated communications links. Such systems are much more vulnerable to attack. In July 2010 it became apparent that one widely-deployed SCADA device – manufactured by Siemens – had a hard-coded default password, making it particularly easy to attack. Just such an attack, Stuxnet,[51] appeared shortly thereafter.[52]

Then we can ask why cyber-war occurs. As with traditional forms of war there are different levels of "intensity" of cyber war. Not all of these types of attacks are going to be directed towards destruction of resources or misdirection during an attack. Some will engage in criminal activities while others will engage in intelligence gathering.[53] In this context, Saad et al. provided a general typology of attacks used between Israel and Hezbollah which provides a starting point for developing a more generalized typology of cyber operations. They argue that there are three dimensions; attacks that focus on strategic objectives, attacks that focus on technical objective, and attacks of a political nature.[54] Cyber weapons include viruses, malware, denial of service, spying, along with jamming and blocking.[55] Schmitt's six criteria could be used to evaluate cyber-attacks; these include severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy.[56] These criteria however are focused on international law issues, which while important must be a secondary consideration when building a typology of cyber operations. Liaropoulos proposes a broad typology including cyber espionage, web vandalism, denial of service, and attacks on critical infrastructure. This provided a more practical approach to defining types of cyber operations but needs to be more fully fleshed out in that denial of service may actually be targeted at critical infrastructure.[57] For smaller nations, or terrorist organizations, the use of Distributed Denial of Service (DDoS) attacks are much cheaper to launch than conventional warfare tools against an enemy possessing greater resources in terms of weapons, money, and troops. Cyber-attack for hire is a lucrative business for those who have been previously overlooked as merely cybercriminals. As noted by many, cybercriminals can become rental cyber warriors.[58] Cybercrime and cyber-attacks may, in the long run, lead to increased cyber-attacks.

A number of cyber-wars have been reported in recent history briefly outlined here. In 1999, the cyber-war between Pakistan and India started when armed forces of both the countries were engaged on the

[50] Peter Sommer and Ian Brown, "Reducing Systemic Cybersecurity Risk", *OECD/IFP Project on "Future Global Shocks"*, Report for OECD Multi-Disciplinary Issues International Futures Programme, 14 January 2011, p. 5. Available at: https://www.oecd.org/gov/risk/46889922.pdf (Visited on 04 January 2018)

[51] For a general but compact glossary on cybernetics, see Andrew F. Krepinevichp, *Cyber Warfare: A "Nuclear Option"?*, Center for Strategic and Budgetary Assessments, Washington D.C., 2012, pp. 180-189.

[52] Nicholas Falliere, "Exploring Stuxnet's PLC Infection Process", 2010. Available at: http://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process, (Visited on 01 February 2018).

[53] Craig B. Greathouse, "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?", In. J.-F. Kremer and B. Müller (eds.), *Cyberspace and International Relations*, Springer-Verlag, Berlin, Heidelberg, 2014, p. 24.

[54] Sabrine Saad, Stéphane Bazan, Lorraine Etienne and Christophe Varin, "Asymmetric Cyber-warfare between Israel and Hezbollah: The Web as a New Strategic Battlefield", Proceedings of the ACM WebSci'11, Koblenz/Germany, 14-17 June 2011, p. 1. Available at: http://www.websci11.org/fileadmin/websci/Posters/96_paper.pdf. (Visited on 18 January 2018)

[55] Ibid., p. 4.

[56] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law*, No. 37, 1999, pp. 885-937.

[57] Andrew Liaropoulos, "Cyber-Security and the law of War: The Legal and Ethical Aspects of Cyber-Conflict", GPSC Working Paper # 7, 2011, p. 2. Available at: http://www.gpsg.org.uk/docs/GPSG_Working_Paper_07.pdf. (Visited on 09 December 2017)

[58] Richard A. Clarke and Rob Knake, *Cyberwar: The Next Threat to National Security and What to Do About It*, Harper Collins, New York, NY, 2010.

battlegrounds of Kargil. In 2003, the US servers were under attack by hackers alleged to be of Chinese origin in order to reveal US government secrets. In April 2007, Estonia's IT infrastructure came under heavy attack by Russian hackers, damaging critical Estonian websites and servers. In December 2007, large number of Kyrgyz websites came under heavy attack during the election campaign. In October 2008, Russia launched a cyber-attack along with a conventional attack on critical Georgian websites and servers disabling their communication and information services.[59]

If we pay first attention on Estonian case, Estonia, which has a population of 1.4 million people including a large ethnic Russian minority, depends heavily on electronic services and that is why Estonia is also known as E-stonia. Estonia has e-government also known as paperless government and even the parliament is elected over the internet. When Estonia was subjected to a barrage of cyber-attacks, it was forced to cut its external Internet connections so that people within the country could continue to use their conventional services.[60] Being highly dependent on electronic services, such a cyber-attack against the country's IT systems can be catastrophic. The cyber-attacks that were carried out were very coordinated and well planned which inflicted chaos across Estonia and Estonia was near to a halt of its critical business processes. Main targets of the attacks were Estonian's presidency and parliament, government ministries, political parties, famous news organizations, banks and communication infrastructure. The attacks were so intensified that Estonia had to block foreign access to sites under siege. Some experts termed it as an onslaught of Estonia and security experts from NATO, European Union, Israel, and USA[61] converged to Tallinn to help Estonia.[62]

As wars historically go, it wasn't very big, did not involve vast amounts of military forces, nor did it last long. One might argue that it was more of a typical battle or campaign framed in an on-going long term geopolitical cold war between the combatants, a cold war punctuated with occasional outbreaks of small to large scale violence. On the surface, it represents one of many cold wars (with periodic renewals of formal national-level military conflict) fought every day on the "near abroad"[63] of peripheries of many states. Thus, for instance, the Russian-Georgian war in August of 2008, a conflict which may not end for a very, very long time, was quite historic and precedent setting for several reasons regarding cyber warfare. But while much of that is true, a deeper analysis of the cyberspace domain operations conducted by all sides in the conflicts indicate that image is illusory and incomplete.[64]

This appears to be the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other war-fighting domains (consisting of Land, Air, Sea, and Space); "*…three weeks before the shooting war between Georgia and Russia began, online attackers started assaulting Georgia's websites. Since then, researchers have tried to find out who masterminded the network strikes - military electronic warriors, patriotic hackers, cyber-crooks - without finding anything definitive.*"[65] Nevertheless, "*…Russia invaded Georgia on four fronts. Three of them were conventional - on the ground, through the air, and by sea. The fourth was new - their attacks via cyberspace ... It is, quite simply, implausible that the parallel attacks by land and by cyberspace were a coincidence - official denials by Moscow notwithstanding.*"[66] The (alleged) Russian attack upon the Georgia's military and government networks was highly successful;[67] "*It seems that 54 web sites in Georgia related to communications, finance, and the government were*

[59] Muhammad Saleem and Jawad Hassan, ""Cyber warfare", the truth in a real case", Project Report for Information Security Course, University of Linköping, Sweden, 2009, p. 1.
[60] Michael Lesk, "The new front line: Estonia under cyberassault", *IEEE Security and Privacy*, Vol. 5, No. 4, July-Aug. 2007, pp. 76-79.
[61] The United States has identified cyber-attacks on its critical infrastructure as a matter of national security, and has declared cyberspace a domain of war. See Robert O'Harrow, *Zero Day: The Threat in Cyberspace*, Diversion Books, New York, 2013.
[62] Saleem and Hassan, ""Cyber warfare", the truth in a real case", p. 2.
[63] David Hollis, "Cyberwar Case Study: Georgia 2008", *Small Wars Journal*, Jan. 6, 2011, p. 1. Available at: http://smallwarsjournal.com/blog/2011/ (Visited on 05 January 2018)
[64] Bob Killebrew, "Russia-Georgia: Early Take", *Small Wars Journal*, Aug. 15, 2008. Available at: http://smallwarsjournal.com/blog/2008/08/russiageorgia-the-impact-first/ (Visited on 14 January 2018)
[65] Noah Shachtman, "Georgia Under Online Assault", *Wired Danger Room Magazine*, 10 August 2008. Available at: https://www.wired.com/2008/08/georgia-under-o/ (Visited on 11 January 2018)
[66] Noah Shachtman, "Top Georgian Official: Moscow Cyber Attacked Us-We Just Can't Prove It", *Wired Danger Room Magazine*, 11 March 2009. Available at: http://www.wired.com/dangerroom/2009/03/georgia-blames/ (Visited on 11 January 2018)
[67] William C. Ashmore, "Impact of Alleged Russian Cyber Attacks", *Baltic Security & Defence Review*, Vol. 11, No. 1, 2009, pp. 4-40.

attacked by rogue elements within Russia ... So as tanks and troops were crossing the border and bombers were flying sorties, Georgian citizens could not access web sites for information and instructions."[68] Georgian authorities discovered their Internet access and communications networks to be exceptional vulnerable to (alleged) Russian interference.[69]

What are some of the operational and intelligence lessons that can be drawn from these cases? (1) First, for Russia or China to employ their people's patriotic 'hacker militia' to conduct a network attack against a target nation-state, they must engage them first - to motivate and 'sell' them on the concept; steer them toward appropriate targets; synchronize those cyberspace operations with combat activity in the physical realm; and discuss the most effective cyberspace tactics, techniques and procedures (TTPs) to be used. Nations need to monitor hacker chat rooms and communications of potential aggressor nations in order to intercept and understand this activity. (2) Second lesson, targets in cyberspace need to be identified and accesses developed prior to any actual military operation. The actual planned attacks and activities need to be practiced at a low level to assess their effectiveness. In future cyber combat, nations will need to conduct these preparatory operations, reconnaissance activities, and probing attacks well in advance of any network attack conducted in support of traditional military operation. There will be an attempt to disguise these activities but it is possible that they can be detected by the target nation networks. (3) Third lesson to be gleaned from this conflict is that the Russian-oriented hackers/militia took out news and local government web sites specifically in the areas that the Russian military intended to attack in the ground and air domains. The Federal and local Georgian governments, military, and local news agencies were unable to communicate with Georgian citizens that were directly affected by the fighting. This provided an intelligence indicator of the ground and air attack locations. It created panic and confusion in the local populace, further hindering Georgian military response. (4) Fourth lesson is that the target nation's patriot hackers/cyber militia will probably be targeted first (or at least early in combat) by an aggressor nation in order to preemptively remove retaliatory capability. There have been a whole series of patriot cyber-militia hacker wars with various levels of government support for their local patriotic hackers over the past 20 years. These individual hackers and cyber-militias target each other and often know each other (at least by reputation).[70]

Those lessons, which were granted from cyber warfare cases occurred in the last two decades as a few was mentioned above in detail, illustrate the requirement for nations that intend to successfully operate in the cyberspace domain to develop air-gapped cyberspace ranges where various scenarios of attack/defend combinations can be practiced and played out in free-play force-on-force combat within a variety of network topology and technology terrain environments. This exercise environment must be integrated with physical domain exercise scenarios in order to better understand the interplay between cyberspace and the physical domains. It also needs to provide a training ground for cyberspace operators to understand and practice the nuances of both offensive and defensive operations (often two separate communities) and how to synchronize cyberspace operations with full spectrum Information Operations (IO) and political/military objectives in the other domains.[71]

4. CYBER WARFARE IN THE 21st CENTURY: THREATS, CHALLENGES, AND OPPORTUNITIES

The impact of the information age on warfare has been a major issue over the last two decades as policy makers, soldiers, strategists, and non-state actors consider how best to use and protect themselves from the threat of cyber war. Unlike weapons of the past, the technology necessary for waging cyber war are not restricted to particular actors within the system. The capacity to assault important systems exists both in state and non-state actors and could possibly cripple whole societies that have become reliant on information. Over the last several years the world has seen examples of

[68] Jon Oltsik, "Russian Cyber Attack on Georgia: Lessons Learned?", *Network World*, 17 August 2009. Available at: http://www.networkworld.com/community/node/44448 (Visited on 11 January 2018)
[69] Ben Arnoldy, "Cyberspace: New Frontier in Conflicts, Internet Attacks on Georgia Expose a Key Flaw for More than 100 natİons", *Christian Science Monitor*, 13 August 2008. Available at: http://www.csmonitor.com/USA/Military/2008/0813/p01s05-usmi.html (Visited on 11 January 2018)
[70] David Hollis, "Cyberwar Case Study: Georgia 2008", pp. 5-7.
[71] Ibid., p. 7.

cyber war. Attacks include the 2007 cyber-attack on Estonia, the 2008 attack on the state of Georgia, the Stuxnet virus from 2009 which attacked the Iranian nuclear program,[72] and the actions by the hacker group "Anonymous" against companies such as Visa, MasterCard, PayPal, and Amazon over the Wikileaks scandal.[73] Each attack illustrates the potential destructiveness of cyber war; "*Because cyber warfare is unconventional and asymmetric warfare, nations weak in conventional military power are also likely to invest in it as a way to offset conventional disadvantages.*"[74] While "bombs" may not be going off with cyber war, the impact of this type of conflict may in fact be more devastating in terms of disrupting societies; "*The more electronically dependent an actor is, the more vulnerable it is.*"[75]

Cyber threats are real and getting worse every year, but they are not as new as we think. Each of the previous cases mentioned above were made about 25 years ago, if not longer. Adversaries in cyberspace and their motivations are no different than in the physical world:[76] cyber-attackers are terrorists; and they act because they lost; because they are behind; because they are so-called revolutionary; because they are starving, and eventually because they hate. By this view, for defense and deterrence regarding cyber warfare in the 21th century, we should thoroughly consider five main issues that stand out with respect to traditional concepts of defense and deterrence: what isn't a problem, how do we respond, what's most different, what we didn't see coming, and what we might most have wrong; "*Deterrence relies on more than the implied threat of the use of force in response to an attack. It requires statements about intentions and understanding among potential opponents that define and limit the environment for conflict. Deterrence in cyberspace is limited because we have not adequately assessed what combination of cyber capabilities, defensive measures, and international agreements will make the United States and its allies most secure. It would be useful to undertake a larger strategic calculation, preferably in a public dialogue, to determine the weighting and balance among offensive, defense and multilateral efforts in cyberspace that best reduces the risk of cyber-attack.*"[77]

In this regard, our first recommendation will be that a government takes further steps to deal with foreign influence. Treating those as "cyber" events misses what makes them unique and brings the wrong set of experts to the table. Frankly, one would have better equipped to handle these challenges in the 1990s when forward-looking officers created doctrines, organizations, and operating concepts around information operations, not just cyber. Even though the military are not the best choice of government agency to respond to other nations seeking to influence or undermine the one's system of government, their capabilities might be built up most quickly. Thus, for any state, a Cyber Mission Force should be organized that would have area-studies specialists working alongside with cyber subject matter experts. A new set of Cyber Influence Teams could be trained as well in this context.

A norms-based deterrence posture has its issues. One is determining how much of a consensus is required to establish a norm. One advantage of working from the UN charter is that UN membership is universal – but the conversion from the words of the charter into the new fields of cyberspace is hardly obvious. Using the threat reprisals to dissuade cyber-attacks introduces multiple issues that need far more careful attention than they have received to date. The notion that building an offensive capability second to none suffices for deterrence is simplistic, to say the least. Granted, weak countries cannot deter. However, many states are by no means weak, especially in cyberspace. If the

[72] Liam O'Murchu, "An in depth look into Stuxnet", 2010. Available at: http://www.virusbtn. com/conference/vb2010/abstracts/LastMinute7.xml. (Visited on 24 December 2017)
[73] Craig B. Greathouse, "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?", In. J.-F. Kremer and B. Müller (eds.), *Cyberspace and International Relations*, Springer-Verlag, Berlin, Heidelberg, 2014, p. 22.
[74] Kenneth Geers, "Sun Tzu and Cyber War", *Cooperative Cyber Defence Centre of Excellence*, 2011. Available at: http://www.ccdcoe.org/articles/2011/Geers_SunTzuandCyberWar.pdf (Visited on 02 January 2018)
[75] Liaropoulos, "Cyber-Security and the law of War…", p. 4.
[76] Jason Healey, "Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities", Hearing on "Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities" before the *Committee on Armed Services, United States House of Representatives*, One Hundred Fifteenth Congress, First Session, March 1, 2017, p. 4.
[77] James A. Lewis, "The "Korean" Cyber Attacks and Their Implications for Cyber Conflict", Center for Strategic and International Studies, Washington, D.C., 2009, p. 5.

one state's deterrence policy has problems they are not ones of weakness but wisdom,[78] notably in determining where to draw the line between cyber-attacks that are actionable at the national level and those that can either be ignored or responded to via judicial processes.[79]

The defining questions for life in the 21st century may be: what is cyber-war? Will we know it when we see it? If so, what do we do in response? The lack of precision in the terminology helps to cloud the issue. Terms such as cybercrime, cyber espionage and cyber-attack are often used interchangeably. We speak of hackers, cybercriminals, and cyber terrorists as if they were identical. In many cases, they may be, or at least they may be closely related. Underlying factors, such as the level of activity or behavior involved in cyber-war, and how many or what type of cyber-attacks it takes for it to be defined as a cyber-war, become important.[80] In recognizing the role that cyber-attacks will play in future military conflicts, two threshold requirements have been identified when nation-states assess the consequences and their potential response. First, what is the threshold for considering a cyber-event an act of war or comparable to the use of force? Second (which will not be addressed in this article), what is the threshold between tactical and strategic applications of cyber-attacks?[81]

This evolution of war is particularly important when addressing cyber-war, which can include both kinetic and non-kinetic activities. Kinetic activities are associated with motion.[82] In the military arena, this typically includes armed attacks, bombs dropping, etc. Non-kinetic cyber-war actions are typically directed towards targeting any aspect of an opponent's cyber systems such as communications, logistics, or intelligence. When used in conjunction with a kinetic battle, non-kinetic cyber activities can include disruption of an opponent's logistical supply chain or diversion of essential military supplies. Other types of non-kinetic cyber activity can include the destabilization of a government's financial system, interference with a government's computer systems, or infiltrating a computer system for the purposes of espionage. The ongoing debate discusses the extent to which these non-kinetic activities should be considered as cyber warfare when they are not associated with an actual physical battle.[83] Then, if we may recount on the heuristic classification of cyber-attacks, we can emphasize that those attacks are launched at multiple levels. This below list is not intended to be hierarchical, or all-inclusive. Among the levels where cyber-attacks can occur are:

- Government versus Government (within the context of a kinetic battle),
- Asymmetrical warfare: Non-state actor versus the agencies or contractors of its own, or another government,
- Government against another Government's critical infrastructure (non-kinetic battle),
- Criminally inspired hackers versus individual users.[84]

Cyber-attacks between nation-states can occur within the context of kinetic and non-kinetic battles. In the case of the nation-state of Georgia, while the cyber-attacks occurred as adjunct to a kinetic war with the Russian Federation, it was believed that Russia had hired virtually every criminal hacker in

[78] Peter Sommer, "The Future for the Policing of Cybercrime", *Computer Fraud and Security*, No. 1, 2004, pp. 8-12.
[79] Greathouse, "Cyber War and Strategic Thought…", p. 22.
[80] Angelyn Flowers and Sherali Zeadally, "Cyberwar: The What, When, Why, and How", *IEEE Technology and Society Magazine*, Vol. 33, No. 3, Fall 2014, p. 1.
[81] James A. Lewis, "Cyberwar thresholds and effects", *IEEE Security and Privacy*, Vol. 9, No. 5, Sept./Oct. 2011, p. 25. See also Peter Sommer, "Intrusion Detection Systems as Evidence", First International Workshop on Recent Advances in Intrusion Detection, Louvain-la-Neuve, Belgium, 1998; Peter Sommer and Gus Hosein, "Briefing on the Interception Modernisation Programme", *LSE Policy Engagement Network*, London, 2009, pp. 1-59.
[82] A blended or combination attack is when a conventional "kinetic" attack is accompanied by a logical attack with the purpose of disorientating victims. In principle this is not new – in kinetic war a routine tactic is to disrupt the radio communications of the enemy by jamming radios and/or creating misleading radio traffic. In today's network-enabled wars the disruption has to be to networks as opposed to radio nets. Operations of the United States and its allies in Kuwait in 1990-91 and Iraq in 2003 were both accompanied by "electronic warfare". During the Georgia/South Ossetia conflict of 2008 there were widespread disruptions of Internet traffic in the region. See Noah Shachtman, "Georgia Under Online Assault", *Wired Danger Room Magazine*, 10 August 2008. Available at: https://www.wired.com/2008/08/georgia-under-o/ (Visited on 11 January 2018). There have also been allegations of Hamas-linked cyber-attacks on Israel in 2008. See Home Security Newswire, "Hamas, Hezbollah Employ Russian Hackers for Cyber Attacks on Israel", *Homeland Security News*, 15 June 2009.
[83] Flowers and Zeadally, "Cyberwar: The What, When, Why, and How", p. 1.
[84] Ibid., p. 20.

Europe, both to assist in perpetrating the cyber-attacks, as well as to deprive Georgia of an opportunity to retaliate in kind.[85] Very few single cyber-related events have the capacity to cause a global shock. Governments nevertheless need to make detailed preparations to withstand and recover from a wide range of unwanted cyber events, both accidental and deliberate. There are significant and growing risks of localised misery and loss as a result of compromise of computer and telecommunications services. In addition, reliable Internet and other computer facilities are essential in recovering from most other large-scale disasters.[86] Therefore, the report prepared by Sommer and Brown in January 2011, as part of a broader OECD study into -Future Global Shocks-, the authors identify the following actions for governments of 21st century:

- Ensure that national cyber security policies encompass the needs of all citizens and not just central government facilities,
- Encourage the widespread ratification and use of the Cyber Crime Convention and other potential international treaties,
- Support end-user education as this benefits not only the individual user and system but reduces the numbers of unprotected computers that are available for hijacking by criminals and then used to mount attacks,
- Use procurement power, standards-setting and licensing to influence computer industry suppliers to provide properly tested hardware and software,
- Extend the development of specialist police and forensic computing resources,
- Support the international Computer Emergency Response Team (CERT) community, including through funding, as the most likely means by which a large-scale Internet problem can be averted or mitigated,
- Fund research into such areas as: Strengthened Internet protocols, Risk Analysis, Contingency Planning and Disaster Propagation Analysis, Human Factors in the use of computer systems, Security Economics,
- Attempts at the use of an Internet "Off" Switch, even if localised, are likely to have unforeseeable and unwanted consequences.[87]

As for today, if we examine level of preparedness by some nations, we come into various parameters which affect the situation. Governments, even in advanced economies, have significantly different levels of preparedness for cyber security risks and attitudes towards dealing with them. For some the response has been to build up military offensive and defensive capabilities on the basis that the main threat is cyber-attack, which they believe can be deterred. Other countries concentrate on mitigation and recovery - the civil contingencies agenda. Such an approach requires the cooperation of the private sector, especially those businesses delivering essential services with whom a particular set of understandings must be evolved. Many states are looking for international agreements on law and declarations of non-use of cyber weaponry. Governments are also developing a role in educating and preparing their citizens.[88]

In this context, first pillar could be military responses against cyber threats. The armed forces of nations such as the US and China have made very significant investments in offensive and defensive cyber-capabilities. The United States Department of Defense established a unified Cyber Command responsible for addressing "a growing array of cyber threats and vulnerabilities" and to "secure

[85] Robert Haddick, "This Week at War: Lessons from Cyberwar I", Foreign Policy, Jan. 28, 2011. Available at: http://www.foreignpolicy.com/articles/2011/01/28/this_week_at_war_lessons_from_cyberwar_i?print=yes&hidecomments=yes&page=full (Visited on 18 January 2018)
[86] Sommer and Brown, "Reducing Systemic Cybersecurity Risk", p. 5.
[87] Ibid., p. 8.
[88] Ibid., p. 61.

freedom of action in cyberspace."[89] In May 2008 NATO established a Co-operative Cyber Defence Centre of Excellence in Talinn/Estonia.[90] The UK House of Lords has urged NATO to work closely with the EU "*...to achieve cooperation rather than duplication.*"[91] In July 2010 extensive news reports said that the Indian Army was developing considerable cyber-war capabilities, principally as a response to perceived threats from China.[92] And for the other pillars in the fight against cyber threats, we could recount on robust national strategies, civilian impact, public-private partnerships, international strategies, possible new technical measures, research and education.[93]

5. CONCLUSION

This study covered in general the realm of cyberspace phenomenon, the motivation and mentality used to carry out cyber warfare attacks. The research tried to create a situational awareness at which point we are by considering along with possible defenses, deterrence, challenges and warfare against cyber-attacks in line with national security. It is difficult to assess with much certainty the likelihood, the character and the consequences of economic cyber warfare, and therefore to gauge the Turkey's vulnerability to such a challenge. This study is, therefore, necessarily speculative. For policy makers seeking to identify genuine security challenges and then to anticipate them, cyber warfare is of doubtful credibility and, consequently, its suitability for the allocation of scarce security and defense resources must be open to question. This essay suggests, nevertheless, that while the idea of cyber warfare might not merit a full-scale policy response at present, it would be prudent to subject it to sustained and careful scrutiny in coming years. Cyber warfare could, in other words, be an ideal candidate for the risk-based approach to national security, risks and challenges in which should be introduced by the government in, somewhat, a national cyber security strategy.[94]

Before we are able to conclude on any conflict conducted on that new battleground represented by the internet, and which is already dominated by the 'fifth element"[95] (after sea, land, air and space), we find ourselves today also having to fight a war of words over the meaning of the term 'cyber-war'. But what is a cyber-war? At what point can we say that we find ourselves facing an electronic war? What are its rules of engagement, and what methods are there for verifying that our responses are commensurate with any attacks suffered? Where can we lay the blame for any attack, and with what degree of certainty? They are questions which, despite being posed at the very dawn of the creation of a specific Cyber Command[96] by the United States Department of Defense (DoD), have still not been answered definitively. They are also questions which are constantly being bandied about as part of this war of words between those who are convinced that the Western world – *in primis America* – has for some time been in the middle of a real cyber-war, which is timeless, normless and unconstrained.

As another conclusive aspect, this study tried to explore how and whether definitions, norms and properties built up based on conventional warfare should apply to cyber-attacks - attacks that may cause substantial, tangible harm but do not resemble a typical act of war like dropping a bomb. Complicating matters further is the difficulty of developing new norms, collaborative fighting-

[89] US Secretary of Defense, "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations", Memorandum dated June 23, 2009. Available at: www.govexec.com/nextgov/0609/gates_cybercommand_memo.pdf (Visited on 23 January 2018)

[90] NATO (North Atlantic Treaty Organisation), "Defending Against Cyber Attacks", May 2008. Available at: www.nato.int/issues/cyber_defence/practice.html (Visited on 23 January 2018)

[91] House of Lords European Union Committee, "Protecting Europe Against Large-scale Cyber-attacks", HL Paper 68, The Stationary Office, London, 2010, p. 26.

[92] Times of India, "Cyber War: Indian Army Gearing Up", 19 July 2010. Available at: http://timesofindia.indiatimes.com/articleshow/6187297.cms?prtpage=1 (Visited on 01 February 2018)

[93] Robert Jervis, "Cooperation under the Security Dilemma", World Politics, Vol. 30, No. 2, 1978, pp. 167-214.

[94] Colin Gray, Modern Strategy, Oxford University Press, Oxford, 1999, pp. 4-5.

[95] For a more in-depth analysis, see, Martin C. Libicki, "Cyberdeterrence and Cyberwar", RAND Corporation, Santa Monica, 2009. Available at: http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf. (Visited on 21 January 2018)

[96] For a more in-depth information on this issue, see U.S. Department of Defense, "Fact Sheet: The Department of Defense (DoD) Cyber Strategy", April 2015, pp. 1-2. Available at: https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/; "U.S. Cyber Command Cyber Guard 15 Fact Sheet", 01 July 2015, pp. 1-4. Available at: https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/; "The Department of Defense Cyber Strategy", April 2015, pp. 1-42. Available at: https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/ (All Visited on 14 February 2018)

techniques and cooperative relations in a challenging domain that is inherently secretive, unpredictable, unlimited and timeless. Thus, we are so vulnerable to its risks and threats.

We propose with this study to distinguish cyber-warfare from other conduct in cyberspace. We should frame possible future prospects of cyber warfare by comparing the strategic, policy and legal questions to those that were facing the world on the eve of a new Cold War between USA and Russian Federation. This comparison can be seen in three ways. First, cyber-war raises strategic questions: Who will be using these cyber-weapons, and how will they be used? Will they be used strategically the way that nuclear weapons have been as a way of shaping or reshaping the global balance of power? What would escalation and deterrence look like in cyberspace? Second, cyber-war raises questions about what institutions will be relevant. The United States, for instance, has taken the lead in this area, as it did during the Cold War. The key institution is the U.S. Cyber Command, which is co-located with the NSA (National Security Agency) and which operates mainly in cyberspace. Third, cyber-war raises legal questions: What counts or what ought to count as a use of force within the meaning of the *jus ad bellum* (the law of going to war) in international law for purposes of cyber-warfare? Should it be a test about breaking things and killing people in the world or should it be some other kind of test? When is an act of self-defense justified in connection with cyber-warfare?[97]

For many states, anxiety over possibility of using information technology systems as an alternative way to procreate a new type of terrorism and spoilage has been a real concern since commencement of information technology systems for the nearly last 50 years of mankind. However, it is interesting to observe that cyber threat became an actuality and genuineness following Estonia cyber assault on April 2007. Though the damages caused by cyber-attacks are yet to be seen but experts believe that such attacks are not as harmful as conventional and nuclear weapons. The cyber-attacks are weapons of mass disruption rather than mass destruction. The cyber warriors are not restricted by geographical boundaries that mean you need a strong defense against an army that is always at our door.[98]

Today, as our Republic prepares to celebrate its centennial, the world is no less tumultuous. There are new actors and new forces in the international system, and the role of technology is unlike anything that could have been imagined in previous years. As our Republic prepares to address these challenges, one of the most important areas of concern is the cyber realm. In recognition of this challenge, our government should establish a Cyber Project. Each year then an International Conference on Cyber Engagement had better convene in order to bring together experts from the public, private, and nonprofit sectors from all over the world to analyze the most critical issues in the cyber realm and think creatively about ways to address problems. And so, if what has been discussed above is correct, at this point it would be particularly difficult to describe this type of threat as having been "overestimated", given the possibility (if not the probability) that the damage that might arise from this threat is not just verifiable, but that it could also put the lives of citizens in serious danger, as this study has shown.

Above all, even the faintest possibility of cyber warfare points to the need for a more agile and mutually supportive relationship between national governments and critical sectors of the economy such as science and innovation, manufacturing and industry, and the financial and banking sector. Otherwise, the first casualties of cyber warfare are likely to be the credibility of national government and the confidence and predictability upon which a national economy depends.[99]

REFERENCES

Books

[97] Harry H. Rimm, Charles Michael and Howard Master (Rapporteurs), "Cyber-War and the Law of Armed Conflict", The United States Courts for the Second Circuit 2014 Judicial Conference on Cyber-Security in the Age of Cyber-Terrorism (11-13 June 2014, Saratoga Springs, New York), *Second Circuit Judicial Conference Report of Proceedings*, New York, 2015, p. 22.
[98] Saleem and Hassan, ""Cyber warfare", the truth in a real case", p. 6.
[99] Cornish, "The Vulnerabilities of Developed States to Economic Cyber Warfare", p. 14.

CARVALHO, F. Duarte and Da SILVA, E. Mateus, Cyberwar-Netwar: Security in the Information Age, IOS Press, Amsterdam, 2006.

CLARKE, Richard A. and KNAKE, Rob, Cyberwar: The Next Threat to National Security and What to Do About It, Harper Collins, New York, NY, 2010.

COLMAN, Andrew M., A Dictionary of Psychology, Oxford University Press, Oxford, UK, 2009.

GOLDSMITH, Jack L. and WU, Tim, Who Controls the Internet?: Illusions of a Borderless World, Oxford University Press, New York, 2006.

GRAY, Colin, Modern Strategy, Oxford University Press, Oxford, 1999.

HUGO, Victor, The History of a Crime, T.H. Joyce and Arthur Locker (trans.), Nabu Press, Charleston, SC, 2010.

JOHNSON, Stuart E. and LIBICKI, Martin C., Dominant Battlespace Knowledge: The Winning Edge, National Defense University Press, Washington, D.C., 1995.

KREPINEVICHP, Andrew F., Cyber Warfare: A "Nuclear Option"?, Center for Strategic and Budgetary Assessments, Washington D.C., 2012.

LESSIG, Lawrence, Code and Other Laws of Cyberspace, Basic Books, New York, 1999.

MAZANEC, Brian M., The Evolution of Cyber War, University of Nebraska Press, Nebraska, 2015.

NYE, Joseph S., Cyber Power, Harvard Kennedy School, Cambridge, MA, 2010.

O'HANLON, Michael E., Technological Change and the Future of Warfare, Brookings Institution Press, Washington, D.C., 2000.

O'HARROW, Robert, Zero Day: The Threat in Cyberspace, Diversion Books, New York, 2013.

OHLIN, Jens David, GOVERN, Kevin and FINKELSTEIN, Claire, Cyberwar: Law and Ethics for Virtual Conflicts, Oxford University Press, Oxford, UK, 2015.

ROBERTS, Adam and GUELFF, Richard, Documents on the Laws of War, 3rd Ed., Oxford University Press, Oxford, 2000.

SCHMITT, Michael N. (Ed.), Tallinn Manual on The International Law Applicable to Cyberwarfare, Cambridge University Press, Cambridge, U.K., 2013.

SINGER, Peter W. and FRIEDMAN, Allan, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, New York, N.Y., 2014.

WIENER, Norbert, Cybernetics or Control and Communication in the Animal and the Machine, John Wiley and Sons, New York, 1955.

Articles, Papers, Reports and Thesis

Additional Protocol 1 (1977) to the Geneva Conventions 1949.

ALFORD, Lionel D., "Cyber Warfare: A New Doctrine and Taxonomy", Crosstalk: Journal of Defense Software Engineering, Vol. 14, No. 4, 2001, pp. 27–30.

ASHMORE, William C., "Impact of Alleged Russian Cyber Attacks", Baltic Security & Defence Review, Vol. 11, No. 1, 2009, pp. 4-40.

BEN-ISRAEL, Isaac, "Security, Technology, and the Future Battlefield," in Haggai Golan, ed., The Texture of Security, Maarachot, Tel Aviv, 2001, pp. 269-327.

BEN-ISRAEL, Isaac, "From the Sword's Blade to Computer Memory", Odyssey, No. 9, October 2010, pp. 4-13.

BLANK, Stephen, "Can Information Warfare Be Deterred?", Defense Analysis, Vol. 17, No. 2, 2001, pp. 121-138.

BRECHBÜHL, Hans, BRUCE, Robert, DYNES, Scott and JOHNSON, M. Eric, "Protecting Critical Information Infrastructure: Developing Cybersecurity Policy", Information Technology for Development, Vol. 16, No. 1, 2010, pp. 83-91.

CETRON, Marvin J. and DAVIES, Owen, "Ten Critical Trends for Cyber Security", The Futurist, Vol. 43, No. 5, 2009, pp. 40-49.

CORNISH, Paul, "The Vulnerabilities of Developed States to Economic Cyber Warfare", Chatham House Working Paper, London, June 2011, pp. 1-15.

CORNISH, Paul and DORMAN, Andrew, "Dr. Fox and the Philosopher's Stone: The Alchemy of National Defence in the Age of Austerity", International Affairs, Vol. 87, No. 2, March 2011, pp. 335-353.

FLOWERS, Angelyn and ZEADALLY, Sherali, "Cyberwar: The What, When, Why, and How", IEEE Technology and Society Magazine, Vol. 33, No. 3, Fall 2014, pp. 14-21.

GJELTEN, Tom, "Shadow Wars: Debating Cyber Disarmament", World Affairs, Vol. 173, No. 4, November/December 2010, pp. 33-42.

GREATHOUSE, Craig B., "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?", In. J.-F. Kremer and B. Müller (eds.), Cyberspace and International Relations, Springer-Verlag, Berlin, Heidelberg, 2014, pp. 21-40.

HEALEY, Jason, "Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities", Hearing on "Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities" before the Committee on Armed Services, United States House of Representatives, One Hundred Fifteenth Congress, First Session, March 1, 2017, pp. 1-35.

Home Security Newswire, "Hamas, Hezbollah Employ Russian Hackers for Cyber Attacks on Israel", Homeland Security News, 15 June 2009.

International Committee of the Red Cross (ICRC), "Cyber Warfare and International Humanitarian Law: The ICRC's Position", ICRC Food-for-Thought Paper, June 2013, pp. 1-4.

JENSEN, Eric Talbot, "Cyber Warfare and Precautions Against the Effects of Attacks", Texas Law Review, No. 88, 2010, pp. 1533-1569.

JERVIS, Robert, "Cooperation under the Security Dilemma", World Politics, Vol. 30, No. 2, 1978, pp. 167-214.

KLIMBURG, Alexander, "Mobilising Cyber Power", Survival, Vol. 53, No. 1, 2011, pp. 41-60.

LESK, Michael, "The new front line: Estonia under cyberassault", IEEE Security and Privacy, Vol. 5, No. 4, July-Aug. 2007, pp. 76-79.

LEWIS, James A., "The "Korean" Cyber Attacks and Their Implications for Cyber Conflict", Center for Strategic and International Studies, Washington, D.C., 2009.

LEWIS, James A., "Cyberwar thresholds and effects", IEEE Security and Privacy, Vol. 9, No. 5, Sept./Oct. 2011, pp. 23-29.

MANSON, III, George Patterson, "Cyberwar: The United States and China Prepare for the Next Generation of Conflict", Comparative Strategy, Vol. 30, No. 2, 2011, pp. 121-133.

MOURA, G. Moreira, "Internet Bad Neighborhoods", Published Doctorate Dissertation, University of Twente, Overijssel, The Netherlands, 2013.

OBAMA, Barak, "Executive Order 13636: Improving Critical Infrastructure Cybersecurity", Federal Register, Vol. 78, No. 33, Part III, Feb. 19, 2013.

PHILBRICK, Ian Prasad (Ed), "International Engagement on Cyber VI: Forum: The Role of Strategy in Securing a Nation in the Cyber Domain", Georgetown Journal of International Affairs, Vol. 17, No. 3, Fall/Winter 2016, pp. 1-109.

RIMM, Harry H., MICHAEL, Charles and MASTER, Howard (Rapporteurs), "Cyber-War and the Law of Armed Conflict", The United States Courts for the Second Circuit 2014 Judicial Conference on Cyber-Security in the Age of Cyber-Terrorism (11-13 June 2014, Saratoga Springs, New York), Second Circuit Judicial Conference Report of Proceedings, New York, 2015, pp. 21-24.

SALEEM, Muhammad and HASSAN, Jawad, ""Cyber warfare", the truth in a real case", Project Report for Information Security Course, University of Linköping, Sweden, 2009, pp. 1-7.

SCHREIER, Fred, "On Cyberwarfare", DCAF Horizon 2015 Working Paper No. 7, The Geneva Centre for the Democratic Control of Armed Forces (DCAF), Geneva, 2013, pp. 1-133.

SCHMITT, Michael N., "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", Columbia Journal of Transnational Law, No. 37, 1999, pp. 885-937.

SOMMER, Peter, "Intrusion Detection Systems as Evidence", First International Workshop on Recent Advances in Intrusion Detection, Louvain-la-Neuve, Belgium, 1998.

SOMMER, Peter, "The Future for the Policing of Cybercrime", Computer Fraud and Security, No. 1, 2004, pp. 8-12.

SOMMER, Peter and HOSEIN, Gus, "Briefing on the Interception Modernisation Programme", LSE Policy Engagement Network, London, 2009, pp. 1-59.

TABANSKY, Lior, "Basic Concepts in Cyber Warfare", Military and Strategic Affairs, Vol. 3, No. 1, May 2011, pp. 75-92.

UK Office of Cyber Security, "Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space", Parliament Command Paper 7642, London, 2009.

WARFIELD, Douglas, "Critical Infrastructures: IT Security and Threats from Private Sector Ownership", Information Security Journal: A Global Perspective, Vol. 21, No. 3, 2012, pp. 127-136.

Internet Sources

ARNOLDY, Ben, "Cyberspace: New Frontier in Conflicts, Internet Attacks on Georgia Expose a Key Flaw for More than 100 natİons", Christian Science Monitor, 13 August 2008. Available at: http://www.csmonitor.com/USA/Military/2008/0813/p01s05-usmi.html (Visited on 11 January 2018)

CORNISH, Paul, LIVINGSTONE, David, CLEMENTE, Dave and YORKE, Claire, "On Cyber War", Chatham House Working Paper, London, 2010. Available at: http://www.chathamhouse.org/ publications/papers/view/109508 (Visited on 28 December 2017)

CRESSWELL, Julia, Oxford Dictionary of Word Origins, "cybernetics." Oxford Reference Online, Oxford University Press, Oxford, UK. Available at: http://www.oxfordreference.com/views/ENTRY.html? subview=Main&entry=t292.e1374 (Visited on 06 January 2018)

DANCHEV, Dancho, "Seven myths about zero day vulnerabilities debunked", 3 August 2010. Available at: http://www.zdnet.com/blog/security/seven-myths-about-zero-day-vulnerabilities debunked/7026?tag=mantle_skin%3Bcontent (Visited on 18 January 2018)

Encyclopædia Britannica, 2010, "space," Encyclopædia Britannica Online. Available at: http:// www.britannica.com/EBchecked/topic/557313/space (Visited on 06 January 2018)

FALLIERE, Nicholas, "Exploring Stuxnet's PLC Infection Process", 2010. Available at: http://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process (Visited on 01 February 2018)

GEERS, Kenneth, "Sun Tzu and Cyber War", Cooperative Cyber Defence Centre of Excellence, 2011. Available at: http://www.ccdcoe.org/articles/2011/Geers_SunTzuandCyberWar.pdf (Visited on 02 January 2018)

GORMAN, Siobhan, "Electricity Grid in U.S. Penetrated By Spies", The Wall Street Journal, 8 April 2009. Available at: http://online.wsj.com/article/SB123914805204099085.html (Visited on 05 January 2018)

HADDICK, Robert, "This Week at War: Lessons from Cyberwar I", Foreign Policy, Jan. 28, 2011. Available at: http://www.foreignpolicy.com/articles/2011/01/28/this_week_at_war_lessons_from_cyberwar_i?print=yes& hidecomments=yes&page=full (Visited on 18 January 2018)

HM (Her Majesty) Government, "A Strong Britain in an Age of Uncertainty: The National Security Strategy", TSO, Cm 7953, October 2010, London, pp. 1-39. Available at: http://www.official-documents.gov.uk/ (Visited on 22 January 2018)

HOLLIS, David, "Cyberwar Case Study: Georgia 2008", Small Wars Journal, Jan. 6, 2011, pp. 1-10. Available at: http://smallwarsjournal.com/blog/2011/ (Visited on 05 January 2018)

House of Lords European Union Committee, "Protecting Europe against Large-scale Cyber-attacks", HL Paper 68, The Stationary Office, London, 2010.

Idaho National Laboratory, "NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses", May 2010. Available at: http://www.fas.org/sgp/eprint/nstb.pdf (Visited on 02 February 2018)

International Committee of the Red Cross (ICRC), "What Limits Does the Law of War Impose on Cyber Attacks?", 2013. Available at: https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm (Visited on 11 January 2018)

KILLEBREW, Bob, "Russia-Georgia: Early Take", Small Wars Journal, Aug. 15, 2008. Available at: http://smallwarsjournal.com/blog/2008/08/russiageorgia-the-impact-first/ (Visited on 14 January 2018)

LIAROPOULOS, Andrew, "Cyber-Security and the law of War: The Legal and Ethical Aspects of Cyber-Conflict", GPSC Working Paper # 7, 2011. Available at: http://www.gpsg.org.uk/docs/GPSG_Working_Paper_07.pdf (Visited on 09 December 2017)

LIBICKI, Martin C., "Cyberdeterrence and Cyberwar", RAND Corporation, Santa Monica, 2009. Available at: http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf (Visited on 21 January 2018)

MELE, Stefano, "Cyber Warfare and Its Damaging Effects on Citizens", September 2010, pp. 1-19. Available at: http://stefanomele.it/public/documenti/185DOC-937.pdf (Visited on 11 January 2018)

NATO (North Atlantic Treaty Organisation), "Defending Against Cyber Attacks", May 2008. Available at: www.nato.int/issues/cyber_defence/practice.html (Visited on 23 January 2018)

OLTSIK, Jon, "Russian Cyber Attack on Georgia: Lessons Learned?", Network World, 17 August 2009. Available at: http://www.networkworld.com/community/node/44448 (Visited on 11 January 2018)

O'MURCHU, Liam, "An in depth look into Stuxnet", 2010. Available at: http://www.virusbtn.com/conference/vb2010/abstracts/LastMinute7.xml (Visited on 24 December 2017)

SAAD, Sabrine, BAZAN, Stéphane, ETIENNE, Lorraine and VARIN, Christophe, "Asymmetric Cyber-warfare between Israel and Hezbollah: The Web as a New Strategic Battlefield", Proceedings

of the ACM WebSci'11, Koblenz/Germany, 14-17 June 2011. Available at: http://www.websci11.org/fileadmin/websci/Posters/96_paper.pdf (Visited on 18 January 2018)

SHACHTMAN, Noah, "Georgia Under Online Assault", Wired Danger Room Magazine, 10 August 2008. Available at: https://www.wired.com/2008/08/georgia-under-o/ (Visited on 11 January 2018)

SHACHTMAN, Noah, "Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It", Wired Danger Room Magazine, 11 March 2009. Available at: http://www.wired.com/dangerroom/2009/03/georgia-blames/ (Visited on 11 January 2018)

SOMMER, Peter and BROWN, Ian, "Reducing Systemic Cybersecurity Risk", OECD/IFP Project on "Future Global Shocks", Report for OECD Multi-Disciplinary Issues International Futures Programme, 14 January 2011, pp. 1-119. Available at: https://www.oecd.org/gov/risk/46889922.pdf (Visited on 04 January 2018)

STAMP, Jason, DILLINGER, John, YOUNG, William and DEPOY, Jennifer, "Common vulnerabilities in critical infrastructure control systems", November 2003. Available at: http://www.sandia.gov/ccss/documents/031172C.pdf (Visited on 14 January 2018)

Times of India, "Cyber War: Indian Army Gearing Up", 19 July 2010. Available at: http://timesofindia.indiatimes.com/articleshow/6187297.cms?prtpage=1 (Visited on 01 February 2018)

UK Cabinet Office, "Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards", 2009. Available at: www.cabinet office.gov.uk/media/349103/strategic-framework.pdf (Visited on 18 January 2018)

U.S. Department of Defense, "Fact Sheet: The Department of Defense (DoD) Cyber Strategy", April 2015, pp. 1-2. Available at: https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/ (Visited on 14 February 2018)

U.S. Department of Defense, "U.S. Cyber Command Cyber Guard 15 Fact Sheet", 01 July 2015, pp. 1-4. Available at: https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/ (Visited on 14 February 2018)

U.S. Department of Defense, "The Department of Defense Cyber Strategy", April 2015, pp. 1-42. Available at: https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/ (Visited on 14 February 2018)

US Secretary of Defense, "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations", Memorandum dated June 23, 2009. Available at: www.govexec.com/nextgov/0609/gates_cybercommand_memo.pdf (Visited on 23 January 2018)

United States Presidency, "International Strategy for Cyberspace", May 2011, pp. 1-30. Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Visited on 29 January 2018)