RESEARCH REPORTS 28

ISIS

# The Changing Balance of Power in the Age of Emerging Cyber Threats

*Ivo Tsekov*

Institute for Security and International Studies

(ISIS)

Sofia, June 2017

**RESEARCH REPORTS 28**

**Institute for Security and International Studies**

**(ISIS)**

**Sofia**



**ISBN 978 - 954 - 9533 – 32 - 3**

**Abstract:** This paper addresses one of the key issues of the international security agenda today: the role of cyber warfare in the changing security landscape of the 21st century. 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 IT means. While a great deal has already been written on the topic, there needs to be a stronger examination of how the combination of cyber weapons with traditional strategic approaches might impact strategic choices related to cyber war. In order to understand whether there is a security competition in cyberspace, it is necessary to assess the current balance of power. Therefore, the issue of cyber warfare has relevance to practitioners, policy-makers, and scholars in the national, regional and international levels.

**Keywords:** cyber warfare, information technology, cyber security, balance of power

## 1. Rethinking Asymmetric Threats

"Cyber warfare" is a recent term: the Oxford English Dictionary gives its first use as 1994. 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 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, and the actions by the hacker group "Anonymous" against companies such as Visa, MasterCard, PayPal, and Amazon over the Wikileaks scandal.[1] More recently, the US Department of Homeland Security and FBI have released an analysis of the allegedly Russian government-sponsored hacking groups blamed for breaching several different parts of the Democratic party during the 2016 elections.[2] Each attack illustrates the potential destructiveness of cyberwar.

[1] Greathouse, Craig B., Cyber War and Strategic Thought: Do the Classic Theorists Still Matter? University of North Georgia, 2014, p.22

[2] FBI and Homeland Security detail Russian hacking campaign in new report, The Guardian, Dec. 29, 2016, https://www.theguardian.com/technology/2016/dec/29/fbi-dhs-russian-hacking-report

Going forward policy makers will be required to develop strategies which address the issues of cyber war. The difficulties of developing effective strategies will be compounded by a multitude of issues including; what qualifies as cyber war, should responses be the same as from attacks by state or non-state actors, does the state respond the same if elements of its private sector are attacked rather than the public sector, and whether an offensive or defense stance is necessary? This paper argues that policy makers do not have to start from scratch in their search for effective strategies. Examining traditional strategic thought will yield possible solutions to the issues of cyber war and state policy. While a great deal has been written on the topic, there needs to be a stronger examination of how the combination of cyber weapons with traditional strategic approaches might impact strategic choices related to cyber war. Are the past approaches to warfare fit for the evolving world of cyber war or must a new generation of strategists be developed to specifically address the ideas of cyber war within the system? Examining the possible applicability of classic ideas of warfare to cyber war must include possible policy ramifications based on potential outcomes.

Although the concept of power acquires new meanings, one could use the phrase "balance of power" - in the classical acceptance of the international relations theory - and in cyberspace. In most senses, simplified, balance of power is aimed at achieving a "parity" of forces/ capabilities in order to avoid the emergence of one side's hegemony and it is done either by "subscription" to an arms race or by rallying to an alliance/ alliance system. Beyond adding a new dimension to the battlefield, cyberspace brings substantial alterations to power characteristics and its manners of manifestation. Therefore, an essential concern, especially regarding cyber warfare, would be: will the state entities continue also to be the main actors for the new cyber environment?

## 2. Achieving balance of power in cyberspace

Cyberspace is becoming the most progressive warfare domain after World War II and all international actors quickly recognize it. In July 2016, during the Warsaw Summit, NATO officially accepted cyberspace as a "domain of operations" and admitted that cyber defense is part of the Alliance's core task of collective defense.[3] Both offensive and defensive cyber warfare capability is a sound strategic balancing factor that potentially will be utilized in any number of future conflicts. The attractiveness of cyber warfare for the weaker state is due to its low cost of development and deployment, its minimum visibility during development and mobilization as a weapon, attribution, globalization of information and global accessibility of technology and the fact that stronger states are more dependent on their critical cyber infrastructure.

[3] NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit, available at http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf

Cyber policy is having trouble keeping up with the changing times; gone are the days when the most significant threat in cyberspace was isolated hackers. Today, cyber policy must contend with sophisticated state actors, and a myriad of non-state actors consisting of transnational crime organizations, hacktivists, and government-employed hackers.[4] In the dawn of the digital age, factors related to economy, certainty, and risk make cyberspace the preferred means of accomplishing one's desired effects in war. To accomplish one's ends, cyber strategy should exploit the capabilities of the targeted opponent's systems. When one's opponent is vulnerable within cyberspace, then the opponents overall dependence on networks and systems should be the governing factor when determining whether to employ cyber as an operational means.

However, whereas many cyber-threats and illicit activities in cyberspace, are everyday's business, most of them do not qualify as a security threat, let alone an act of war. Instead, the present research aim to focus solely on states and state policy in cyber space where the concept of cyber power revolves around the low barriers to entry and relatively limited cost of exerting influences on many facets of a society, from war to commerce.[5]

The cyber domain is a unique case where the more you have invested and expanded on your capabilities in cyberspace, the more vulnerable you are.[6] Globalization - fueled by technological advancement and spread of cyber space in physical space- is a manifestation of new means through which power is exercised and distributed. On the same token such power comes with a vulnerability that states such as North Korea and China are trying to separate themselves from by keeping their critical infrastructure isolated from internet reach. The exponential growth of internet and dependence of our critical infrastructure to cyber space (i.e. power grids, emails, emergency systems, reconnaissance networks, military communication, weapons, etc.) begs the question; can cyber warfare be the dominant dimension for interstate conflicts in the future?

One may argue that U.S. being a more wired state, and arguable the strongest state by far from its rivals in technology also holds a strong ground in cyber defense. But it is important to note that the inherent characteristic of the cyberspace favors the attacker, not the defender. Or better, the prospect of the attacker being successful against given targets is higher than the prospect of the defender thwarting the aggression.[7] Furthermore, unlike conventional or nuclear war, a cyber-attack is not always obvious. It may take years to identify an attack and by that time the source of attack may have been disappeared from the cyber space. Further, from a defensive perspective, it is difficult to imagine how to defend a space that has no boundaries. Also, based on its design, internet changes constantly, grants access to anyone, and exists virtually

[4] Kelly, Terrence K. and Jeffrey Allen Hunker, Cyber Policy, Journal of Law and Policy for the Information Society, 2012, p. 216
[5] Eidman, Christopher R., p.16
[6] Paganini, Pierluigi, Cyber warfare – Cyber Space and the status quo balance of power; dichotomy or symphony?, February 2015, available at http://securityaffairs.co/wordpress/33448/cyber-warfare-2/cyber-warfare-balance-of-power.html
[7] Locatelli, Andrea, The Offense/Defense Balance in Cyberspace, October 2013, p.10, available at http://www.ispionline.it/sites/default/files/pubblicazioni/analysis_203_2013.pdf

everywhere. If offense is seen as cheaper, and defense is seen as expensive, actors within the system may remain more likely to strike out against others for both gain and as a preemptive measure. Even if states or actors do not perceive the balance accurately, it still affects their behavior, because their behavior is based on their perception of the balance.[8] In cyberspace this problem remains, but is compounded by the fact that there is currently little perceived risk in cyber-attacks. Added to the balance misunderstanding, there is also little risk if an attack fails making the potential "cost" of offense even lower.

As a result, achieving balance of power on this newly-found domain is complex and daunting task.

Cyber warfare capability as a strategic weapon for countries such as North Korea seems to be their most viable option. The low cost of entry (for example, a personal computer connected to the Internet), and the ability to operate anonymously, and the problem with attributing an attacker to a cyber-attack are factors that makes cyberspace attractive to adversaries who know they cannot challenge the United States in a symmetrical contest. Potential adversaries, such as China, Iran and North Korea, are reportedly developing capabilities to attack or degrade U.S. civilian and military networks.[9] In a conventional warfare scenario, deterrence has an important role. Fear of retaliation makes the attacker to pause and rethink its actions. In the case of cyber warfare, deterrence has not been an effective strategy for the U.S. and it seems that no other country, nuclear power or not, is exempt from this. The problem with deterrence is that countries are not equally vulnerable to cyber-attacks, thus cyber retaliations or balancing will not be the same as equalization of nuclear warfare capabilities. The aim of deterrence is to create disincentives for starting or carrying out further hostile action however in the case of cyber-attack this notion is hard to achieve. Deterrence also requires the adversary to be able to distinguish between being punished from not being punished. In most realms this is not a problem, however for cyber warfare this is a major problem. There, the higher the penalty for any one cyber-attack, the greater the odds that the punishment will be viewed as uneven. This by nature can be contributed to the attribution problem inherently embedded in the cyber warfare capability.

Therefore, it is imperative for the international community to consider cyber warfare as a viable and dangerous weapon for rogue states and those actors that need its capabilities to gain economic and political advantage against the dominant political structure. The current balance point is not a final state. It can be argued that unlike physical weapon systems infrastructure, the cost to adjust software is minuscule. In a number of respects, it is significantly cheaper to make changes in cyberspace.[10] These changes may provide an opportunity to adjust the balance more

[8] Lynn-Jones, Sean M. Offense Defense Theory and its Critics, Security Studies 4, no. 4 (1995), p.660–691
[9] Ibid.
[10] Malone, Patrick, Offense-defense balance in cyberspace: a proposed model, December 2012, Monterey Naval Postgraduate School, p.66

in favor of defense. In the end, the hereby proposed model is not good or bad. It is just an estimate of where cyberspace currently sits.

### 3. From risk to threat - evaluating security in cyberspace

Cyber-security problems call for new critical approaches to understanding technological and societal risks emerging from this area, and future policy challenges can only be addressed when we identify the nature of the problem appropriately. Cyber-security is considered a growing political, economic and social threat, which is constantly evolving and challenging high-tech users globally. The way in which security is understood has developed rapidly over the last century, and this has had an influence on the recent risk-based security paradigm. As with traditional forms of war there are different levels of "intensity" of cyberwar. 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 intelligence gathering while others will provide false information aimed at destabilizing or misleading society. Due to the nature of the of this evolving realm of conflict they would all fall within cyber operations but an effective typology must be constructed to provide guidance to policy makers and strategic thinkers about how to address certain types of attacks.

During the Cold War, threats were defined militarily from external sources. As a result, threats activated a defense mechanism to protect the sovereign state. In this hostile environment, new directions in security studies slowly began to emerge, including non-military security issues. The definition of threat and security has changed over the years, but it is generally understood a threat to be an action or sequence of events that threatens drastically and over a relative brief span of time to degrade the quality of life for the inhabitants of a state.[11] This is a very comprehensive definition, and it is still functional in the current security climate because it defines a variety of threats or risks that a nation could face at any given time without focusing solely on exceptional measures.

New types of security threats have emerged during the 21st century, which circumvent the traditional analysis in the threat-security tandem. The current security paradigm calls for a different management structure based on resilience and preparedness linked to risk-management and anticipatory governance and practices. The most recognized new area is cyber-security, which has had an impact on all levels of everyday life, i.e. public and private sectors, and groups and individuals. The way in which cyber-security is conceptualized and managed cannot be comprehended in an analytical framework where exceptionalism is central. Cyber-security often fails to be categorized by its normal or exceptional nature. Anew dynamic develops from the global interconnectivity and dependency on computer technology, because computers are common almost in everyday life and as a result, new threats have surfaced.

[11] Ullman, Richard, Redefining Security, International Security, Vol. 8, 1983, p.129

Saad et al. (2011) 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.[12] Conversely, Schmitt's (1999) six criteria could be used to evaluate cyberattacks; these include severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy.[13] Finally, Liaropoulos (2011) proposes a broad typology including cyber espionage, web vandalism, denial of service, and attacks on critical infrastructure.[14]

Tabansky (2011) proposes that hostile activity in cyberspace should be ranked according to types of activity undertaken and damage caused. What follows is a proposed classification, arranged in descending order of severity.

a. An attack on various civilian targets that causes physical damage.

b. Disruption of and attack on critical national information infrastructures, which causes physical damage.

c. Disruption of and attack on military targets in the state's sovereign territory.

d. Disruption of and attack on military targets outside the state's sovereign territory.

e. Insertion of dormant attack tools, e.g., a Trojan horse or logic bomb that are likely to be preparations for an attack.

f. Criminal activity, industrial espionage.

g. Use of dual use weapons: intelligence gathering, probing for common security vulnerabilities, penetration tests.

h. Conducting a propaganda media campaign, abuse and defacement of official websites.[15]

In the 21st century, it has become clear that cyber warfare adds a new dimension to military security and warfare strategies. Cyber-security is the response to the growing threat of cyber-related crimes, and the concept has developed to provide a safe and secure computing environment for all users. Various international and national institutions have failed to develop a comprehensive definition of cyber-security.[16] Cyber-security can be seen as an umbrella term for

[12] Saad, S., Bazan, S., & Varin, C., Asymmetric cyber-warfare between Israel and Hezbollah: The web as a new strategic battlefield. Proceedings of the ACM WebSci'11, 2011
[13] Schmitt, M., Computer network attack and the use of force in international law: Thoughts on a normative framework. Columbia Journal of Transnational Law, 1999, 885–937
[14] Liaropoulos, A., Cyber-Security and the law of war: The Legal and Ethical Aspects of Cyber-Conflict. GPSC Working Paper # 7., 2012, available at http://www.gpsg.org.uk/docs/GPSG_Working_Paper_07.pdf
[15] Tabansky, Lior, Basic Concepts in Cyber Warfare, in Military and Strategic Affairs, 2011, p.82
[16] Munk, Tine, Cyber-security in the European Region: Anticipatory Governance and Practices, University of Manchester, 2015, p.47

numerous, differentiated and fragmented security risks, all of which share one common factor: the use of cyber-space and the Internet. The definitions above show that the field is too complex for one security actor to deal with. Cyber-space is an area where a limited number of activities are visible, and control of the Internet is almost impossible. In the contemporary world, there is a complicated and self-sufficient digital underground economy in which data is the unlawful product.

The most common terms used to distinguish different types of unlawful online activities are cyber-crime, cyber-warfare and cyber-terrorism. A cyber-related crime could be an organized cyber-attack using malicious software or malware in the form of viruses, worms, Trojan horses or logic bombs.[17] The important factor is to look at the underlying motives to determine whether an attack is carried out for economic or personal gain, is part of an important cyber-warfare campaign/information-warfare or is based on political, religious or ideological reasons. Cyber-attacks follow technical innovations, with the denial-of-services (DoS) and distributed denial-of-services (DDoS) being the most common. The DoS and DDoS attacks attempt to make a machine or network resource unavailable to its intended users by exhausting their resources, i.e. overloading the mailbox or the website by redirecting overwhelming traffic to it.

Cyber-terrorism is the use of different computer networks to harm/shut down critical infrastructure, to spread propaganda, or to communicate.[18] The growing dependency on information technology gives the terrorists a chance to approach targets, which otherwise would be out of their reach. The more dependent the public-private sectors have become on technology, the more vulnerable it will be to future cyber-attacks. However, this area is not clearly defined because often there is no identifiable actor that characterizes cyber-terrorists, nor is it possible to pinpoint their activities.[19] The people involved in cyber-terrorism can be rough states, terrorists, disgruntled insiders, private companies and political activists.

The most typical of these offenses are attacking targets that deliver critical infrastructure, disruption of financial transactions, theft of secret information, and crippling the transport system. Another area of cyber-terrorism is introducing malware or hacking sensitive areas of critical infrastructure in order to obtain confidential information through espionage. Cyber-terrorism has been characterized as a new form of war, which we only understand in vague terms. Daily life revolves around the digital world, using the Internet, computers and mobile phones. As a result, it is expected that the providers of devices, Wi-Fi and broadband take steps to maximize the protection against attacks, and there is a similar expectation towards governments and security institutions that they will do the same. Although there has not been a significant cyber-terrorism event so far, it has become an increasing problem in relation to spreading propaganda and hiring jihadists for Islamic State (ISIS) in Syria and Iraq. This terrorist organization openly uses the Internet to raise awareness and distribute its ideology to young

[17] Ibid., p.49
[18] Weimann, Gabriel, Cyberterrorism: The Sum of All Fears?, 2005, p.129
[19] Jordan, T. and Paul A. Taylor, Hacktivism and Cyberwars: Rebels with a cause?, 2004, p.39

people through web pages and social media. Moreover, ISIS uses social media to distribute images of their atrocities, such as the beheadings of hostages. The Internet is the primary facilitator for spreading propaganda and communication, and it can be a powerful tool for mobilisation and radicalisation. However, the actions of terrorist organisations are impossible to measure, and no one knows the scale of the use of the Internet as a communication tool between terrorists and/or other organised crime groups.[20]

Unauthorized access to computer information resources is common to every kind of cyber threat. However, the unauthorized intrusion into a computer information resource opens a broad spectrum of possible results. What is the extent of the threat from the various actors? Are all the actors and the threats relevant to national security? How can we assess their importance and prioritize the response policy? A public discussion is needed in order to provide a serious answer to these questions.

Up to this point strategic approaches which point to offensive types of operations have been examined. The question becomes can defense and deterrence be a viable policy stance for states? Defense is the ability to actively resist if an attack is launched against an actor. 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.[21] 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. However, given the need for interconnectiveness, segregating most systems from the ability to communicate defeats the purpose of connectivity. Some defenses that can be put into place include encryption, firewalls, and automated detection. But as with most defenses these are as good at the updates and operators, and even then can still be penetrated.

Another issue in developing a defensive posture for an actor in the cyber world is what to defend. If a state were only to defend its networks, that may be feasible but that then leaves whole segments of infrastructure which are operated by the private sector open to assault which could have a debilitating impact on society. Even though the private sector does build in defenses against types of cyber threats, an intentional attack is very likely to disrupt their business. In many western states, especially within the United States, private industries are essential in protecting important systems from a cyberattack. This means that any type of strategic defence against cyberattacks must be developed, established, maintained, and coordinated between the government and the private sector.

---

[20] Munk, Tine, Ibid., p.57

[21] Cornish, P., Livingstone, D., Clemente, D., & Yorke, C., On cyber war, 2010, Chatham House, available at http://www.chathamhouse.org/publications/papers/
view/109508.

Risk assessment is a wide and varied field used in various professions, and a professional discussion of it is beyond the scope of this article. In order to formulate policy, we need to assess the threat, i.e., the scenario that makes a policy necessary. An approach to cyber warfare resembles an approach to any new weapon system.[22] In order to assess the relative weight of the cyber threat in the framework of war, familiar variables such as effective range, extent of destruction by the attack, cost of use, political limitations on use, and others must be examined. The cyber threat has the potential to be realized independently of the traditional security system. Cyberspace as it exists today is a wild battlefield. It makes possible direct transfer of data and commands while disregarding national and geographic borders and defensive arrays. As opposed to space, air, land, or sea, existing security organizations are only starting to function in cyberspace. There is a critical potential in cyberspace to undermine national security while bypassing traditional national defense frameworks and directly hitting critical targets on the home front. Thus, the developing phenomenon of cyberspace is creating a strategic change in the field of national security.

## 4. Legal and Ethical Aspects of Asymmetric Cyber Warfare

The examination of the legal, ethical, and attribution considerations and how they may apply to Asymmetric Cyber Warfare is key for understanding this emerging threat. Particular consideration should be paid to how Asymmetric Cyber Warfare could be viewed by the international community and how it may fit into current and future international law.

With the ever increasing reliance on computers and networks for day to day operations, both in the civilian and military sectors, it has become increasingly important to gain a legal understanding of how cyber operations will be viewed in terms of international law. It is widely recognized that attacks within the cyber realm can be of strategic, operational, and tactical importance. Within the legal framework, there is a distinction between cyber-crime (only non-state actors, violation of criminal law), cyber-attack (objective to undermine function of computer network, must have political or national security purpose), and cyberwar (objective to undermine function of computer network, must have political or national security purpose, equivalent to armed attack or occurring during armed conflict).[23]

There is an ongoing debate as to whether cyberspace requires its own body of law or if instead existing law applies to cyberspace.[24] Cyber-attacks, under certain conditions, may be considered a use of force, and therefore prohibited within the UN Charter, with the exceptions of self-defense, and UN Security Council mandate. Controversy arises when discussing state responsibility for acts committed by non-state actors and also acts that do not result in injury or

[22] Tabansky, Lior, Ibid., p.87
[23] Hathaway, Oona et al., The Law of Cyber-Attack,California Law Review, 2012, p.817
[24] Schmitt, Michael N., International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed, The Harvard International Law Journal Online 54, 2012, p.17

damage, as evidenced by the allegations of Russian involvement in the US presidential campaign in 2016.

Parallel to the growing interest in the legal aspects of cyberwar, are an increasing number of questions focused on the ethical dimension. The ethics concerning asymmetric cyber warfare can be incorporated into existing discussions on the moral principles governing conduct in war, and need not be broken out into a unique area for consideration. The main question would be: can computers be used as weapons? Similar to the argument that objects with the capability to cause harm or death are not all categorized as weapons, the argument can be made that the intent of employment of a tool, in this case a computer, to create foreseeably harmful consequences is the means by which computers earn weapons status and the employment of them against an adversary may be considered a use of force.[25]

Some experts observe that, all other things being equal, cyber weapons are less risky to military personal because of the operational distance that can be achieved with their employment, and because cyber weapons can deliver kinetically equivalent military objectives without necessarily resulting in loss of life to one's adversary, nor to innocents and non-combatants.[26] Cyber-attacks can be employed to mitigate the associated collateral damage because of two key factors: targeting precision and repair mechanisms. Target precision provides the means whereby attacks are limited not only by the specificity of the target machines, but also by an advanced level of specific critical software aspects on these machines. The use of repair mechanisms allows for implementation of attack vectors that are easily reversible, either by doing no real harm or only temporary disabling enemy military and critical infrastructure.

The case for the morality of cyber weapons is not without its problems, mostly related to the difficulties associated with identifying attackers and targets and the secrecy associated with conducting cyber-attacks. Technology allows for the near complete anonymity of actors in the cyber domain and severely hampers identification efforts. Typical computer networks are not designed with easy identification in mind.[27] In some instances, the networks' own capabilities unintentionally complicate the act of attribution because of the ease by which information, such as sender addresses can be "spoofed". While possible to improve the attribution process via technological features like logging, tracing, and unique communication keys, these options alone may not be sufficient to provide identification in some cases.

Since the ethics of using cyber weapons is questionable, states might be able to create better regulatory framework and enact an ethical cyber policy by doing one of three things: 1) pledge to never employ cyber weapons, 2) pledge to not use cyber weapons as a first strike capability, or

[25] Bayles, William, Moral and Ethical Considerations for Computer Network Attack As a Means of National Power in Time of War, .S. Army War College, 2000, p.9
[26] Denning, Dorothy and Bradley J. Strawser,Moral Cyber Weapons: The Duty to Employ Cyber Attacks, in The Ethics of Information Warfare, 2012, p.87
[27] Wheeler, David and Gregory N. Larsen, Techniques for Cyber
Attack Attribution, Institute for Defense Analysis, 2003, p.1

3) pledge to only use cyber weapons in response to cyber weapons.[28] As such, the topic or cyber weapons regulation is comparable to the need for regulation of other major weapon systems like nuclear, chemical or biological. The current legal and ethical framework for conducting a just war is as applicable for this type of employment of forces as it has been for the employment of other weapons of scale. The advantage to examining these issues within the existing legal and ethical framework is that the international community would work with familiar concepts and values that have successfully governed the rule of war for decades. As for the global level, a solution such as the development of an international Internet "governance" system under the aegis of International Telecommunication Union, in conjunction with signing an international agreement similar to those of conventional/nuclear arms control but focused on "cyber weapons" within UN could provide an adequate description of the system "status" at a moment in time or the identification of its potential future trends. In the same time, international law must define more sharply the criteria that characterize cyber-attacks as equivalent to armed attacks. It must evolve and adapt, because cyber-warriors have taken the threat out of the realm of the abstract and made it real.

## 5. Conclusion

Cyber capabilities are different from conventional military power in that they are relatively cheap to develop and deploy. This enables weaker states, through the use of offensive cyber warfare, to change the balance of power in their advantage. And cost is not the only benefit to cyber warfare. Plausible deniability is another one. Cyber-attacks are typically carried out by government-funded hackers. Even if the source of an attack is uncovered, the government responsible can deny its involvement without any consequences. Information technology is the nervous system of the global economy. Critical infrastructure for banking, power, transportation, and industry increasingly depends on embedded computers connected to the internet. Firms and citizens entrust vital personal, medical, and financial data to distant servers in return for more convenient and efficient services. Military command and control relies on digital networks to connect far-flung surveillance and strike systems and to project power rapidly and precisely. Yet this vital interconnectivity also facilitates new modes of crime, protest, espionage, and warfare. Ubiquitous computer networks both provide access to valuable targets and become targets themselves. Protecting and influencing cyber infrastructure has thus become a major priority for governments and other political actors around the world.

Few security issues have captured the attention of the public as has the specter of cyberwar. Rapid changes due to technology have increasingly impacted the security environment and military affairs. Information technology is one of the primary change agents in the military of today and likely of the future. With the rise of the networked society, the days of combatant

[28] Rowe, Neil, Ethics of Cyber War Attacks, in Cyber Warfare and Cyber Terrorism, 2008, p.107

forces conducting operations in the physical world alone have gone. In an age of new threats, new and even revolutionary technologies, and new forms of military operations, the requirement for clear thinking increases commensurately. Information about threats is not enough; indeed, the enhanced capability for data retrieval obligates us to understand our enemy as never before. Carefully delineating and understanding the difference between so-called asymmetric threats and asymmetric strategies becomes more important than ever in the current environment.

There needs to be significant work done at all levels of the emerging field of cyber war. There is a need for both strategic thought but also tactical innovation but at the same time these two levels must be able and willing to talk to each other. The human-built world is becoming more complex and more vulnerable. Technology has changed mankind itself and equally so it will change the way mankind wages war. Eventually the nature of war and security will change.

## ABOUT THE AUTHOR

Ivo Cekov (b. 1981) is an M.A. in International Relations, M. A. in International Security and PhD holder in International Relations at the Law School of Sofia University "St. Kliment Ohridsky". His research interests are in the fields of nuclear deterrence, security and cyber security policy. Assistant Professor at the Department of International Relations of the Law School of Sofia University "St. Kliment Ohridsky" and Associate of ISIS since 2016.

## ABOUT THE INSTITUTE FOR SECURITY AND INTERNATIONAL STUDIES (ISIS)

The Institute for Security and International Studies (ISIS) is a non-governmental non-profit organization, established legally in November 1994. It organizes and supports research in the field of security and international relations. Fields of research interest are: national security and foreign policy of Bulgaria; civil-military relations, democratic control of the armed forces and security sector reform; European Integration, Euro-Atlantic security and institutions; Balkan and Black Sea regional security; global and regional studies; policy of the USA, Russia and the other centers of power in international relations; information aspects of security and information warfare; quantitative methods and computer simulation of security studies; theory and practice of international negotiations. ISIS organizes individual and team studies; publishes research studies and research reports; organizes conferences, seminars, lectures and courses; develops an information bank and virtual library through the Internet; supports younger researchers of security, and develops independent expertise in security and international relations for the Bulgarian civil society. The institute networks internationally and establishes links with academic organizations and official institutions in the country and abroad on a cooperative and on a contract basis. ISIS is not linked to any political party, movement, organization, religious or ideological denomination. The institute has a flexible group of voluntary associates – four senior research fellows, six PhD holders, two PhD writers and two MAs – ten altogether.

## PUBLICATIONS OF ISIS

# Research Studies:

***"Bulgaria and the Balkans in the Common Foreign and Security Policy of the European Union"*** *(Plamen Pantev, Valeri Rachev, Venelin Tsachevsky), 44 pp., July, 1995.* Research

Study 1. In Bulgarian and English.

***"Problems of Civil-Military Relations in Bulgaria: Approaches to Improving the Civilian Monitoring of the Armed Forces"*** *(Plamen Pantev, Valeri Rachev, Todor Tagarev), 96 pp., April, 1996.* Research Studies – 2. In Bulgarian.

***"Bulgaria and the European Union in the Process of Building a Common European Defence"*** *(Plamen Pantev, Valeri Rachev, Tilcho Ivanov), 51 pp., September 1996.* Research Studies – 3. In Bulgarian and English.

***"Strengthening of the Balkan Civil Society: the Role of the NGOs in International Negotiations"*** *(Plamen Pantev), 24 pp. ,March 1997.* Research Studies – 4. In Bulgarian and English.

***"The New National Security Environment and Its Impact on the Civil-Military Relations in Bulgaria"*** *(Plamen Pantev), 50 pp., May 1997.* Research Studies – 5. In English.

***"Prenegotiations: the Theory and How to Apply it to Balkan Issues"*** *(Plamen Pantev), 24 pp., October 1998*. Research Studies – 6. In English.

***"Balkan Regional Profile: The Security Situation and the Region-Building Evolution of South-Eastern Europe"*** *(Plamen Pantev, Valeri Rachev, Tatiana Houbenova-Delisivkova), 17 pp., April 1999*. Research Studies – 7. In English (only an electronic version).

***"Black Sea Basin Regional Profile: The Security Situation and the Region-Building Opportunities"*** *(Plamen Pantev, Valeri Rachev, Tatiana Houbenova-Delisivkova), 17 pp., April 1999.* Research Studies – 8. In English (only an electronic version).

***"Security Risks and Instabilities in Southeastern Europe: Recommended Strategies to the EU in the Process of Differentiated Integration of the Region by the Union"*** *(Plamen Pantev), 36 pp., November 2000.* Research Studies – 9. In English (only an electronic version).

***"Civil-Military Relations in South-East Europe: A Survey of the National Perspectives and of the Adaptation Process to the Partnership for Peace Standards"****, in cooperation* 19 *with IIF, Vienna and the PfP Consortium of Defense Academies and Security Studies Institutes, (Plamen Pantev ed.), 218 pp., April 2001,* Research Studies – 10. In English.

***"The Evolution of Civil-Military Relations in South East Europe: Continuing Democratic Reform and Adapting to the Needs of Fighting Terrorism"****, ISIS, Sofia/NDA,*

*Vienna/DCAF, Geneva, Plamen Pantev, etc (eds.), 276 pp. (Hardcover), July 2005, Springer Verlag, Heidelberg,* Research Studies – 11. In English.

***"Bulgaria in NATO and the EU: Implications for the Regional Foreign and Security Policy of the Country"*** *(Plamen Pantev), 28 pp., September 2005, Research Studies – 12. In English.*

***"Post-Conflict Rehabilitation: Lessons from South East Europe and Strategic Consequences for the Euro-Atlantic Community"*** *(Plamen Pantev, Jean-Jacques de Dardel, Gustav Gustenau - Eds.)*, National Defense Academy and Bureau for Security Policy of the Austrian Ministry of Defence, ISIS *Research Studies – 13.* Vienna and Sofia, 2006, *235pp.*

***"U.S. Relations in the Age of Obama"*** *(Plamen Pantev),* in: A. Wess Mitchell and Ted Reinert (Eds.), "U.S.-Central European Relations in the Age of Obama", CEPA Report No 22, July 2009, pp. 23-25. ISIS *Research Studies – 14.* Also available online at: http://www.cepa.org/Publications, July 2009.

***"Joint task Force East and Shared Military Basing in Romania and Bulgaria" (****Plamen Pantev et al),* Occasional Papers Series, George C. Marshall Center, No. 21, August 2009, 23 pp. ISIS *Research Studies – 15.* The paper is also available at: www.marshallcenter.org/occpapers-en, September 2009.

***"Rehabilitation and Multi-stakeholder Partnerships on Security in Post-Conflict Situations: the Case of Afghanistan and Consequences for the European Union",*** *(Plamen Pantev, Velko Attanassoff ),* St.Kliment Ohridski University Press, ISIS *Research Studies–16,* Sofia, *2*010**,** 200 pp.

***"European Union Borders in the Face of Insecurities",*** *(Mira Kaneva), ISIS Research Studies – 17*, Sofia, October 2016.

***"The Inflated Yet Unsolvable North Korean Nuclear Threat",*** *(Boyan Boyanov), ISIS Research Studies – 18 , Sofia, November 2016.*

# Research Reports:

***"The Balkans in the Cooling Relations Between Russia and Western Europe"*** *(Dinko Dinkov), 29 pp., November 1995.* Research Reports-1. In Bulgarian.

***"The Political Dialogue Between the European Union and the Central and Eastern European Countries"*** *(Vladimir Nachev), 15 pp., November 1995.* Research Reports- 2. In Bulgarian.

***"The Bulgarian Foreign Policy in the Post-Conflict Period: Tendencies, Roles, Recommendations"*** *(Plamen Pantev, Valeri Rachev, Venelin Tsachevsky, Tatiana Houbenova-Delisivkova, Dinko Dinkov), 35 pp., November 1995.* Research Reports-3. In Bulgarian.

***"The Bulgarian Military Education at a Crossroads"*** *(Todor Tagarev), 29 pp., September 1996,* Research Reports-4. In English.

***"An International Methodology for Evaluation of Combat Capabilities of Military Systems: the Bulgarian Perspective of Greater Transparency and Confidence"*** *(Volodya Kotsev), 13 pp., October 1996,* Research Reports-5. In English.

***"Confidence and Security in the Balkans: the Role of Transparency in Defence Budgeting"*** *(Tilcho Kolev), 22 pp., November 1996,* Research Reports-6. In English. *20 pp.*

***"NATO Enlargement: Two Looks from Outside"*** *(Laszlo Nagy, Valeri Ratchev), 82 pp., February 1997,* Research Reports-7. In English.

***"Bulgaria and NATO: 7 Lost Years"*** *(Jeffrey Simon), Translation from English into Bulgarian from "Strategic Forum" 142, May 1998, 15 pp., November 1998,* Research Reports – 8. In Bulgarian.

***"Reengineering Defense Planning in Bulgaria"*** *(Velizar Shalamanov, Todor Tagarev), 28 pp., December 1998*, Research Reports – 9. In English.

***"Peacekeeping and Intervention in the Former Yugoslavia: Broader Implications of the Regional Case"*** *(Plamen Pantev), 17 pp., November 1999,* Research Reports – 10. In English.

***"The Emergence of a New Geopolitical Region in Eurasia: The Volga-Urals Region and its Implications for Bulgarian Foreign and Security Policy"*** *(Nikolay Pavlov), 23 pp., December 2000,* Research Reports - 11. In English.

***„Regional Identity in the Post-Cold War Balkans"*** *(Dimitar Bechev), 22 pp., August 2001,* Research Reports – 12. In English.

***„The Balkans and the Caucasus: Conceptual Stepping Stones of the Formation of a New Single Geoeconomic, Geopolitical and Geostrategic Region"*** *(Plamen Pantev), 8 pp., November 2002,* Research Reports – 13. In English.

***"Control, Cooperation, Expertise: Civilians and the Military in Bulgarian Defence Planning Expertise"*** *(Todor Tagarev), 19 pp., April 2003,* Research Reports – 14. In English.

***"Bulgaria's Role and Prospects in the Black Sea Region: Implications of NATO and EU***

***Enlargement"*** *(Plamen Pantev), 12 pp., August 2004,* Research Reports – 15. In English.

***"Euro-Atlantic and Euro-Asiatic Concerns of an Enlarged Europe – a Bulgarian View"***

*(Plamen Pantev), 7pp., August 2004,* Research Reports – 16. In English.

***"Security Threats and Risks in South Caucasus: Perceptions from the Western Black***

***Sea"*** *(Plamen Pantev), 12 pp., June 2005,* Research Reports – 17. In English.

***"The 'Europeanisation' of National Foreign, Security and Defence Policy"*** *(Plamen*

*Pantev), 11 pp., November 2005,* Research Reports – 18. In English.

**"*Initial Impact of the Democratic Protests in the Arab World for the Middle East Peace***

***Process"*** *(Boryana Aleksandrova), 20 pp., September 2011,* Research Reports – 19. In English.

***"The Western Balkans After Mladic, International Relations and Security Network"*** *(Plamen Pantev), 16 June 2011,* Research Reports – 20. In English.

**"*Turkey Looks Ahead"*** *(Plamen Pantev), 29 June 2011,* Research Reports – 21. In English.
**"*Macedonia Eyes Its Future in Antiquity"*** *(Plamen Pantev), 15 August 2011,* Research Reports – 22. In English.

**"*The Black Sea: A Forgotten Geo-Strategic Realm"*** *(Plamen Pantev), 13 October 2011,* Research Reports – 23. In English.

**"*The US/NATO ABM Defense Shield in the Black Sea Region"*** *(Plamen Pantev), 08 December 2011,* Research Reports – 24. In English.

***"The Tensions Between Serbia and Kosovo – A Major Generator of Instability in the Region"*** *(Petyo Valkov), January 2012,* Research Reports – 25. In English.

**"*Media-International Relations Interaction Model"*** *(Tsvetelina Yordanova), December 2012,* Research Reports – 26. In English.

***"The New Challenges to the Euro-American Relationship: Russia and the Middle East"*** *(Amb. Ret. Guido Lenzi), November 2014,* Research Reports – 27. In English.

**Note: Most of the publications in English have electronic versions at the Institute's website:**
**http://www.isis-bg.org**

**ISIS Post-Address:** 1618 Sofia, P. O. Box 231, Bulgaria

**Phone:** ++359888289605

**E-Mail Address: isis.pantev@gmail.com**

**Website: http://www.isis-bg.org**