CYBER WAR – TRENDS AND TECHNOLOGIES

Dr. Darko Trifunović*

Zoran Bjelica**

---

* Prof.Dr. Darko Trifunović, Director of the Institute for National and International Security, professor at Faculty of Law, Administration and Security, Megatrend University, Belgrade. Dr Trifunovic was elected as guest professor at FUDAN University – Center of American Studies, Shanghai, China. Senior Research Fellow and lecturer at Faculty of Security Studies-University of Belgrade. He is Senior Adviser at the Research Institute for European and American Studies, Greece, Athens. He is a specialist in Security studies, Intelligence & Counterintelligence studies as well as Counter-Terrorism, National and International Security studies. He is a former diplomat (First Secretary of the Foreign Service of Bosnia and Herzegovina at the United Nations). Dr. Trifunovic is the representative for Serbia and Montenegro of International Strategic Studies Association (ISSA); Defense & Foreign Affairs publications; and the Global Information System and he is member of the Advisory Board of the Institute of Transnational Studies, Munich, Germany. The Shanghai Center for International Studies appointed him as the first foreign expert for the Olympic Games (2008) security preparation in China. In 2010, he is engaged in World Expo Security preparation and is a Member. Dr Trifunovic is regular speaker at International Counter Terrorism Institute, Tel Aviv, Israel, and Prof. dr Darko Trifunovic is one of the founding Members of the International Counter Terrorism Academic Community (ICTAC). He has published numbers of academic books papers and articles.

** Zoran M. Bjelica, Data Scientist, technical expert in the field of Big Data Analytics and Information Systems Security. As a pioneer in the new scientific discipline of data science, he interdisciplinary approached the definition of fields that use scientific methods, processes, algorithms and systems to extract knowledge and insight from many structural and unstructured data in the field of information security. Activities and field of scientific and professional work is Big Data Analytics, which is based on data mining, machine learning and systematization of large amounts of data. Zoran M. Bjelica is the founder of the Vinča Data Analitika. A special area of expertise is mIOT (Medical Internet Of Things). He has been a lecturer at the Department of Biomedical Engineering at the Faculty of Mechanical Engineering in Belgrade for many years. He has been interested in computer and network systems for over 40 years. He is the author of several scientific monographs, treatises treatises and scientific papers in the field of information security. The Institute for Standardization of Serbia, under his expert supervision

DOI: https://doi.org/10.37458/nstf.21.3.2

Abstract: Cyberspace has become an indispensable part in which special operations such as cyber war or warfare take place. The role of special war as the use of so-called soft power was emphasized. The country's number of potential adversaries in cyber warfare is unlimited, making highly endangered aspects of cyber civilian infrastructure, which is essentially military readiness, including the mobilization of forces through the civilian sector, also a likely target. A special type of cyber war or warfare is hybrid warfare. This type of warfare is increasingly resorted to because it is extremely cheaper than the conventional method of warfare and at the same time brings exceptional results. The first thing that affects cyber security policy analysts comes with the issue of neutrality, as well as the huge variety of assessments about future attack and defense technologies. There is also a consideration that the new (problematic) cyber technology will be deployed in a short period of time, in time periods,

and guidance, adopted the first version of the Serbian Standard SRBS 27001. He is one of the first Internet users in this area who had a professional obligation to test the first Internet academic network.

in just a few days in terms of warnings. Second, is the trends in cyber-attack and defense technologies and who is following those processes. Third, decision making technology having in mind high-performance computers, technologies that are well known, although rapidly evolving, are increasingly seen as a basic means of managing cyber defense at the national military and security level, as well as a new weapon in the hands of opponents. Fourth, role of intelligence in planning future scenarios for defense against hybrid or any other cyber threat/s.

Key words: Cyber war, new technologies

Introduction

In military theories, cyberspace is designated as the fifth combat space next to water, air, land, and space[1]. We are witnessing a great expansion of the fifth combat space, which knows no borders, fences, social or cultural barriers. This space directly enters the privacy of each individual and with powerful techniques as well as analytical programs, "learns" all habits of the user. In 2009, Martin Libicki, one of the most prominent scientists of cyber warfare, concludes in a report he wrote for the US Air Force ("United States Air Force) that

1. Laurence Ifrah, “States face new challenges from cyberwarfare and cybercrime”, Revue Défense Nationale, Vol. 714, 2008.

"the strategic doctrines of cyber warfare are unlikely to be decisive" and that "the operational level of cyber warfare plays an important role in the future".

In 2012, Thomas Reed and Peter McBurney of King's College London noticed an important difference between target-specific cyber weapons, which can be of great value in terms of effect and broader applications, which are in comparison, lower in value than the effect achieved. They point out that there is a clear link between weapon making and high value that "increases the resources, intelligence and time required for development and implementation" which will "likely reduce the number of targets" and "political utility of cyber weapons". These assessments were made based on trends; however, trends must be interpreted in relation to the definitions of “cyber warfare” or “cyber weapons”. Libicki gave a definition of cyber warfare as a directed and individual war (does not include "real" war, only virtual, not physical), and Reed and McBurney define cyber warfare as "computer code used or designed to be used, with the aim of that it is a threat or provocation of physical conflict, that it is functional and that it destroys a structure, system or manpower[2]. "Cyber warfare is an integral part of Special War or Special Warfare. This type of warfare is the use of so-called "soft power". These are some of the main features of special warfare:

2. Thomas Rid, Peter McBurney, Cyber Weapons, The RUSI journal, Volume 157, 2012 - Issue 1, pp.6-13. https://www.tandfonline.com/doi/full/10.1080/03071847.2012.664354 retreived 12.01.2020.

SOFT POWER

- Use of force in international relations - basic definition of power and force;
- Politics from a position of force;
- Forms of use of force in international relations - economic means (restriction of foreign trade, economic measures), political means (enemy propaganda, ideological pressure, psychological warfare, terrorism, spheres of interest);
- Information operations and strategic communications - Objectives of action, Significance and levels of execution, Stages of implementation and levels of operations, Content and methods of implementation, Forces for execution, Means for application of psychological operations, Principles of execution (planning, execution stages, intelligence, implementation), Effects of operations (evaluation and correction).

An important type of information operations is cyber warfare. There are at least three important dimensions to the problem of possible cyber warfare without such estimates being taken into account:

- Will the cost / benefit ratio in technical development and

advanced use of cyber weapons be more favorable over a period of 10-20 years?

- Will the political character of progress in the field of cyber weapons in countries initiate the accumulation of entire cyber arsenals, rather than individual cyber weapons?
- Will the political character of progress in the field of cyber weapons distance countries from conventional military strategies in the information age, through a strategy in which the dominance of information achieves a decisive advantage and capability? The answer to all three questions would be yes.

In time, the conclusions drawn by Libicki, Reed and McBurney will probably be less relevant. For the purposes of discussion and analysis of the national strategy, we must point out the very dynamic character of the area that represents a possible cyber war. As a country of accumulated capabilities, technological capabilities and options in the IT sector, we need to recognize and recognize the real and key interests of most governments of developed countries and their efforts to resolutely move towards information domination, as a strategy of possible cyber war. Proper and timely consideration of our own real possibilities (from technical to organizational) can be a decisive advantage in preventing or reducing the harmful consequences of cyber attacks on our information systems, critical infrastructure or vital functions of the state / society. In cyber

warfare, knowledge and human resource capabilities are a key advantage, perhaps even superiority.

One of the best descriptions of the dynamics of change may be the book "America of the Vulnerable" by Joel Brenner, former inspector general of the US National Security Agency, who takes a highly non-technical approach to the political and economic foundations of war and strategy[3]. We will illustrate the previous points with the basic elements from our knowledge of how China reacted to the United States and its capabilities for information operations, starting with the first Gulf War in 1991, with in-depth attention to cyber fire. This is essential for understanding that cyber warfare technology and strategy are made possible by information domination!

One of the essential conclusions of Brenner's book is that cyber warfare as a real life phenomenon (involving budgets, soldiers, politicians, industries and war / battle) is currently in its infancy and that it could soon be a very real threat. Brenner concludes that his country "cannot defend its electronic networks controlled by energy companies, prevent air crashes, enable reliable financial transactions or allow the president to communicate with his cabinet at the level of secure communication." The country's number of potential adversaries in cyber warfare is unlimited, making highly endangered aspects of cyber civilian infrastructure, which is essentially military readiness, including the mobilization of forces

3. Joel Brenner, America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare, Penguin Press, 2011.

through the civilian sector, also a likely target. ("Electronically Undressed").

If the United States cannot defend its critical infrastructure in cyberspace at the moment, and it turns out that it cannot, if the world is on the brink of rapid expansion of cyber warfare and the capabilities of potential cyber aggressors against Serbia, implications for Serbia and the government that needs to become aware e and at this point we have no answers to such a scenario. Brenner emphasizes a package of policy measures, most of which are very reasonable. While little deals with issues of combat capability of war or strategy, all resources represent potential contributions to national security readiness in cyberspace. For example, he calls for the need to move towards a highly secure computer system (Secure Computing or the use of "proven software" programs) through the promotion and public support of high demands in this area.

The implications of such a transition can be summed up in the claim that governments tolerate too long exposure to their security and the vulnerability of national information systems[4]. A study by the East West Institute called on governments to "send clear signals to enable IT innovation and security drive, starting from the top down, with the highest security requirements and the highest value goals." More importantly, the Institute called on governments to "cooperate internationally and quickly grasp this new paradigm and stop the development of top-notch cyber-attackers

4. Ibid.

before more damage is done[5]." We can also notice the contrast of three assessments which are a real indicator of the difference between the advanced aspect of planning and the backward aspect, precisely on the example of Serbia: "Serbia has not yet been subjected to any activities that could be considered a cyber-attack"; "Strong cyber defense will enable a high degree of trust in networks and information security"; "The fact that in 2014, for the first time, destructive cyber attacks were carried out on American soil, on national / state authorities of the USA" warns that "we must be ready for large-scale disasters - the so-called cyber Armageddon "or that" unpredictable instability is the new norm "and that cyber threats have been realized" of low intensity on the network of nation states, that information conflict is becoming the rule, not the exception "(From the report of the University of Georgia Tech - Georgia Institute of Technology for 2015[6].)

The differences between the first assessment and the other two are more than visible. The Serbian doctrine seems to reduce to the postulate “when the country is not attacked, the country is safe and secure in cyberspace.” Is that so? assessments from American sources painted a completely different picture: Serbia was probably attacked without knowing it (the attack is still going on ?!), so it is no longer safe, it is probably much less safe than the United

5. EestWest Institute, Annual Report 2020, https://www.eastwest.ngo/sites/default/files/ideas-files/ewi-2018-annual-report.pdf
6. Emerging Cyber Threats Report 2015, The Georgia Institute of Technology, https://www.cc.gatech.edu/sites/default/files/images/2015emergingcyberthreatsreport.pdf

States, and Special features of cyber war Leaving aside the great powers and their preparations for cyber war, for a moment, there are other important political and strategic aspects of the war in cyberspace, which are important regardless of the country and which will also develop - probably in the next 10-20 years. Serbia should also take these aspects into account. First, there is the new potential that cyberspace offers for an asymmetric war of weak military forces (and non-state actors) against states that are clearly superior in the conventional military sense[7].

Although this concept has been present for a long time, it is not a static phenomenon, but it is changing with the progress of technology. Asymmetric warfare is the first of three possible military threats facing the United States. The other two are strategic threats from weapons of mass destruction and threats of regional conflicts. Asymmetric threats are defined in the United States as those in which "state and non-state opponents avoid direct engagement with the U.S. military but use new strategies, tactics, and improved weapons of" lateral "technologies to minimize U.S. strengths and exploit perceived weaknesses[8]."

7. Darko Trifunović, International Security and Asymmetric Threats, Asymmetry and Strategy, University of Defence Strategic Research Institute & National Defence School, Belgrade, Serbia, 2018.pp.47-62
8. Franklin B. Miles, Asymmetric Warfare: An Historical Perspective, US Army College, Carlisle Barracks, Pennsylvania, 1999. p.2

There is a constant threat of "cyber war" all over the world, and this threat is the first on the list of threats. Secondly, there is the possibility of "transmitting" the war, ie. there is an ability (and practice of the experienced) that will become increasingly important over time. Simply put, a transferred war is the transfer of war at the national level of the coercive power of either the state or an individual to initiate individual actions and reflects the decentralization of political power. There are several ways to understand this phenomenon in relation to military applications. One is to look at the role of patriotic hackers, whose potential in war can be compared to partisan forces capable of interfering with the enemy, but who are either loosely connected to their command or not connected at all, often acting against its interests or expressions.

Patriotic hacking is an important and developed phenomenon in Serbia, but also in the world, primarily in China, South Korea and Japan, USA.... Another dimension of the transmitted war is the contribution and role of cyber militias, people who have a civilian day job, but who, under the direction of national security, can participate in national security activities in the short term, including cyber war if necessary. As already mentioned, China has an active program for the development of cyber special units, but it also relies on its unique political system in companies.

The United States does not have such explicit reliance on cyber special forces, in part because it has an established network of high-tech companies that can be quickly and easily co-opted into national security activities if needed. It is estimated that there are at least

10,000 "clean" companies with secret technical aspects of intelligence needs. These forms of transmission of war are a sufficient challenge for national security activity. Confirmation of this allegation is the Snowden affair, in which one of those employees was able to use his individual "Network Power" and explode by opening up some of the most sensitive aspects of cyber warfare capabilities and preparation. With Snowden's revelation of "Operation Prism", which involved nine leading U.S. corporations in direct and large-scale engagement in U.S. national security missions in cyberspace, it did even more damage in the end in which these companies reacted by distancing themselves from either which political subordination or participation in the national distribution of cyber war. Microsoft, for example, has clearly defined its position to treat all customers equally, including the United States and China. But the biggest challenge is the transfer of war, and there is a fundamental change in the relationship between the central command and its deployed units.

In an era of information domination and concrete enemy plans to cut off command and control, either through cyber or kinetic means, all military units must now have ways to reconnect if major links in the central chain are broken down. As already mentioned, China has responded to this much more clearly than most countries in its recent military strategy (May 2015).

It also announces the weakening of the central command authority in order to nurture the conditions for winning the cyber war under the motto "self-dependence" for certain military units ("fight your way" and "I fight for my way").

One of the political consequences of the distribution of warfare and their asymmetric potential is that it can also break the traditional value of military alliances, especially the provisions of extended intimidation. Serbia benefits from the technical support of its intelligence allies, preparing for cyber warfare and conducting an information operation. Serbian forces also enjoy significant integration into advanced command structures and control arrangements. There is, however, significant evidence to suggest that the reliance of a middle power, such as Serbia, on alliances between states for prolonged deterrence may not have as much impact in cyberspace as it does on kinetic operations. The United States has agreed with NATO partners that an attack in cyberspace could constitute an armed attack for the purpose of calling for a mutual response under Article 5 of the treaty.

The question is, however, whether the cyber intrusion of a belligerent character or preparatory for war, in practice, will attract the support of the United States within the NATO alliance. It is more than likely that middle-power allies in the United States will have a greater degree of self-confidence in cyberspace than in maintaining the kinetic capabilities of military cooperation because recognizing thresholds for intrusion or attack in cyberspace is far less determined and developed and much more ambiguous than in kinetic. scenario.

There is little room for doubt about the intentions when several bombers of one country violated the airspace of another without prior approval. This would pose a danger of an armed attack. The same clarity does not yet exist for a cyber attack. One should always be

careful here, because Russia's cyber attacks on vital countries of their interest have always preceded kinetic force. This is what happened in the case of the Russian aggression on Georgia. A massive cyber attack was carried out in preparation for a tank invasion[9].

Future attack and defense systems

Trends in cyber attack and defense technologies have been described in many publications: by government agencies, scientists, experts, but also by hackers. They are of importance for the needs of benchmarking ("benchmarking") of national security, and range across all eight base vectors in the "cyber color", but they also include those that reduce and combine individual vectors. This could be called "system of systems" technology. The scale of the challenge in predicting attack and defense technologies should not be discouraged by anyone's misunderstanding of cybersecurity. The first thing that affects cyber security policy analysts comes with the issue of neutrality, as well as the huge variety of assessments about future attack and defense technologies.

There is also a consideration that the new (problematic) cyber technology will be deployed in a short period of time, in time periods, in just a few days in terms of warnings. From the point of view of benchmarking Serbia for the needs of national security, this discussion discourse

9. Paul B. Rich, Crisis in the Caucasus: Russia, Georgia and the West, Routledge, New York, NY, 2010. p.128

carries only a few ideas about future systems that are not particularly pronounced in the public debate by officials or among experts in Serbia. If you look closely at the horizon of specialists from a typical security point of view, characterizing the development of threats around complex cyber attacks is a useful place to start. In 2015, U.S. analyst Karl Herberger, vice president of Security Solutions, reported that in 2013, the average cyber attack included seven vector attacks (although some attacks were over 25 vector attacks), different phases (each with several waves), with successive phases and relying on the methods they performed in the previous phase, but by adding new vector attacks[10].

The following attack vectors are most often mentioned:

1. Compromise of personal data such as passwords and passwords.
2. Weak passwords, passwords and those that can be easily predicted.
3. Malicious insiders, usually referring to employed insiders within a company or institution.
4. Non-existent or poor data encryption.
5. Incorrectly configured system.
6. Cyber extortion, exists when the user is denied access to data by the attacker and is asked for a certain amount of money to access. 7. “Phishing” is a method used by cybercriminals to trick a

10. Carl Herberger, How to Defend Against Hacktivists, Information Security Media Group, 2013. https://www.bankinfosecurity.com/how-to-defend-against-hacktivists-a-5948

user into accessing their personal information, such as a bank account.
8. Trust relations, exist when trust between users or systems develops to a certain extent[11].

In addition to vector attacks, four characteristics in the emergence of threats can be isolated: coordinated persistent threat of actors, dynamic polymorphic malware, multi-vector attacks and multi-phase attack. These characterizations are very important indicators, but they do not warn us how careful we must be. On the one hand, they deal only with a limited part of the attack vector, and do not say much about the defense system.

As one of the leading international examples of future defense systems, we can look at how critical infrastructure protection is recognized by recognized world leaders in cyber defense, the Idaho National Laboratory (INL), which emphasizes that the focus is not military battlefield systems, but also defines many standards. for the development of combat systems and for the creators of the doctrine of defense, as well as cyber leaders who must be able to not depend on a certain critical infrastructure. After all, there is no victory in war without preserved critical infrastructure. And when we talk about the terrorist threat that is more and more present, a special danger arises when terrorists gather information related to critical infrastructure, which allows them to detect vulnerabilities and set targets.

11. 8 Common Cyber Attack Vectors and How to Avoid Them, Balbix. https://www.balbix.com/insights/attack-vectors-and-breach-methods/

From airports and other transport-related infrastructure to society-critical electricity and water supply systems (including nuclear power plants), serious damage to critical infrastructure can cause direct and indirect large losses, including loss of life[12]. We can take the case of power supply, which is only one of the eight vectors of cyber security. This system, although under the management and control of digital assets, also mostly ignores the vector of attacks and responses in cyberspace. This was the subject of testimony by INL Director Brent Stacey on 21 October 2015, who emphasized that any country considering cybersecurity has significant cause for concern due to the following facts:

- The assumption that the control system is “manual” or. that such a system is not an effective cyber security strategy.
- Intrusion detection technology is not well developed for network system control; the average length of time to detect an attack / intrusion is four months and is usually identified by a third party.
- As the complexity and "connection" of system control services increases, the probability of unplanned system failures

12. B. Todorović, D. Trifunović, Security Science as A Scientific Discipline - Technological Aspects, Security Science Journal, No. 1 (2020), Belgrade, Serbia, 2020. p.13 http://www.securityscience.edu.rs/index.php/journal-security-science/article/view/7/1

increases, which is an uncontrolled consequence - independence from malware.

- A dynamic threat develops faster than a cycle of measures and countermeasures, and far faster than the evolution of doctrine.
- The need for trained cyber security, with knowledge of system control, far exceeds our current readiness.

The type of defensive response cited in the professional literature is also instructive[13]. It is an identified approach in three points:

1. Hygiene: "the foundation of our nation's proactivity, composed from day to day, applied measures and counter-struggles"; "important routine tasks such as standards, compliance, password sharing and management"; "with the role of industry in agreement with property owners."
2. Advanced permanent threat: "more sophisticated cyber weapons" require a "strategic cyber partnership with industry and government." This level of partnership in Serbia is still in the process of development, so cyber

13. Greg Austin, Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security, Australian Center for Cyber Security, pp.19-20 https://www.unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/DISCUSSION%20PAPER%20Middle%20Powers%20REARMED%2027%20Jan%202016.pdf

> defense is possible through critical capacity and a wave of reactions by issuing warnings of current vulnerabilities to owners of public and private funds “
> 3. High impact low frequency events:" catastrophic and potentially cascading events they require a lot of time for assessment, response and recovery. This level is primarily the responsibility of government and institutions. “

Research has focused on the two highest priority levels (# 2 and # 3 in the list above), with the aim of establishing a“two to four year cycle of research-to-deployment ”and to“ achieve transformations of innovation that improve the security of our infrastructure forces by reducing complexity, implementing cyber-information design, and integrating selected digital enhancements. "Laboratories" have the great challenge of developing new and deployable solutions to remove the high-value infrastructure asset from the table as a cyber target. " paradigm shift in the methods used for the historical development of the control system”.

This paradigm is based on the fact of traditional trust and relationships in communication are no longer a satisfactory assumption[14]. Instead, the resilient design of control systems expects a malicious attack or action to be a mask of normal operation and designed for the ability of the system to be in action to prevent or mitigate such actions. Serbia does not have a comprehensive procedure to respond remotely according to the set principles of cyber

14. Ibid.

developed countries, and in fact a lot of effort has been made on the lowest priorities (# 1 on the list above) in which the hygiene of operators and companies in cyber security is identified.

Analysis of Great Britain in 2012 provides some additional insights into threat processes and cyber resilience of another aspect of critical infrastructure, financial services financial vector. The study is based on consultations with the economy. Three main aspects are considered, among others. The Internet will become increasingly central in our economy and our society. First, the growing role of cyberspace has also opened up new threats as well as new opportunities - we have no choice but to find ways to address and overcome these threats if the UK wants to grow more economically in a competitive and globalized world. Second, the digital architecture we now rely on is built to be efficient and interoperable. At the beginning of the creation of the Internet, security aspects were not or were less considered. However, as we use the Internet more and spend a good part of our lives on this network, the issue of security has become more and more important. People want to make sure that networks that support our national security, our economy and prosperity, and our own privacy as individuals are secure. Third, unfortunately, an increasing number of threats come from those who use cyberspace to steal, who seek to compromise or destroy personal information. Cyber attacks can affect our critical infrastructure, our workplaces and ultimately our homes. It is for these reasons that the UK National Security

Strategy 2010 has made this threat a “Level 1” threat of the highest priority[15].

Academic studies on a similar topic warn of the danger of underestimating risk and isolation: "Assessing the risk of naive aggregation of risks due to its high reliability and safety and failures according to the 'do not catch on' model." This is called a “biased security choice” model that “reduces the effectiveness of security defenses”. Looking to future doctrines, cyber security is exposed to complex risks, about which very little is known despite their great importance.

Decision-making technologies

High-performance computers, technologies that are well known, although rapidly evolving, are increasingly seen as a basic means of managing cyber defense at the national military and security level, as well as a new weapon in the hands of opponents. Sandia Laboratory sets up and develops future "decision-making technologies" based on high computing performance. It would be useful for Serbian commands (in considering their strategic weapons, including indicators and warnings) to understand these aspects in the vector of analogies and attempts to create an advantage in cyberspace, as a global civilian domain, to the extent of global strategic systems.

15. The UK Cyber Security Strategy Protecting and promoting the UK in a digital world, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

The study sets as the principle core of operational claims that cyber security is a terrain for national decision-making and that it represents a "continuous life cycle with human, organizational, legal and technical interdependencies." It identifies seven high priorities, "broad area problems" in the field of cyber security, which are of great importance in medium intensity and potential for a country like Serbia, in understanding its technology for deciding on a possible cyber war.

These problems and priorities, listed literally, are as follows:

1. Unrelated wide-ranging response and multi-targeted attack;
2. Widespread and fragmented detection of notifications and opportunities;
3. Poorly defined state, trade and academic roles and responsibilities;
4. Divided and rigid doctrine in the broad field of cyberspace protection;
5. Unresolved area of single and joint risk;
6. Fragile and interdependent deployment of a broad approach to critical approach and operations;
7. Unresolved review, attribution of attacks and compromises.

The authors concluded, proposing areas for further research in computer performance, to promote the decision on national security or. decision for cyberspace. It is not surprising that US state laboratories have the scope of work and enormous resources to deal with such challenges, in contrast to scientists who belong to the middle cyber forces who are not

supported by their governments and do not have the same opportunities.

As for Serbia, in the absence of public announcement of a range of similar activities at the strategic level of warfare, we can probably conclude that the scope and means for such an analysis, and subsequent actions, are negligible. Serbia has well-developed research resources in the application of high computer performance, but in the absence of public records, it could be concluded that they are not adequately applicable to cyber activities, especially to the requirements of deciding on a possible cyber war at the strategic level. If we analyze the ecosystem of possible threats and defenses, which stem from a mere "handful" of technology trends (and responses to those trends), it can only be concluded that small and mid-level powers like Serbia are looking at a pipe of almost insurmountable challenges, unless they are trained to develop complex appropriate decision-making systems for medium-level cyber warfare, dealing with simultaneous multi-vector, multi-threat and multi-spatial cyber-attack from an identified enemy, including against civilian infrastructure and civilians in cyber warfare. And all that needs to be protected now before we start thinking about new technologies such as quantum computer systems, biocomputers, anti-satellite weapons, mass deployment of bots as deployed units in space, return to traditional communications for cyber activities and laser-based communications.

Scenario and planning for a possible cyber war

There are many components of planning, financing and training for defense forces for the

future in cyberspace. One of the most important is intelligence, which is the basis for answering the questions:

- What other countries are cyber threats, what are they doing and planning to do?
- What would they do in certain circumstances based on what we know?
- How would future technologies affect their military strategies?

These are some of the topics of the necessary re-examination of Serbia. An additional tool is scenario development, which is especially useful in the context of uncertainty about intelligence services, because this is certainly more than possible in cyber warfare. The value of planning in a cyber war and the feasible scenario is highly valued, especially since the plans of a possible cyber war of potential opponents of Serbia, and even the plans of its allies, will probably remain non-transparent.

The planning benefit and the simulation scenario indicated the need for strict control. There are classic elements of surveillance, such as elucidating possible scenarios of geopolitical activities, but also aspects of cyberspace and scenarios for their ability to extort alternative responses in future technologies and in creating incentives for change among doctrine creators. In the mentioned analysis, the authors also refer to the values that give a common "language" and

doctrines of approach to possible future trends in cyber warfare.

Above all, the authors of the analysis recommend the use of scenarios as a concrete preactive means of reducing strategic surprise ("Reducing the impact of uncertainty through the notion of robustness"). Most major powers have been involved in planning scenarios for civilian cyber emergencies. They have published few details of the scenario for a cyber-possible war, but there is data for a demonstration scenario. As one example, in late 2014, the U.S. government conducted an exercise, the “Cyber Flag,” on a number of non-public ownership scenarios and elements.

Among the scenarios were:

- A joint force to respond to regional crises involving significant military cyber activity;
- Full range of military operations of combat cyber targets;
- Alliance of cyber operations from the air, land and naval forces;
- Simulation of cyber attacks and analysis of the impact on national command and control.[16]

This form of exercise and simulation is very useful, but like most exercises, it is specific to

16. ‘Cyber Flag’ Exercise Tests Mission Skills, From A U.S. Cyber Command News Release,US Dpt.of Defense, 2014. https://www.defense.gov/Explore/News/Article/Article/603637/

training and has developmental benefits that should be limited to the developmental stage of the forces involved in the exercise and do not reflect the overall cyber war situation. military planners at the executive level of government will plan and prepare.For the purpose of assessing the best international practice in the development of scenarios, ie planning for unforeseen cyber warfare, it would be important to undertake more detailed studies, because no prospect of a possible cyber war in Serbia has been sufficiently analyzed and assessed.

But for the purposes of this paper, it may be sufficient to emphasize that defense planning at the national level, with respect to future cyber warfare, is crucial. Either we will be a "kingdom of the blind" if Serbia does not build the capacity for opposition, or these capacities will be built at all levels of the state and society. One of the most discussed examples in the United States is the case of the military conflict with China over Taiwan. This is an example that is very credible and includes a wide range of cyber attacks against American civilian infrastructure in order to prevent the mobilization of American forces or to delay their deployment in the Western Pacific.

For a country like Serbia, the list of possible cyber threats and attacks is long:

- Cyber-hybrid threats to Europe,
- Cyber-hybrid threats to Serbia,
- Cyber-criminal gangs ,
- Individual cases of cybercrime or
- Cyber terrorism.

Consideration of such scenarios leads us to only one of three possible conclusions about Serbian doctrine. First: the medium intensity of a possible cyber war is known and in such a scenario we have to make the necessary planning. Or else: we have not studied enough to know whether national consensus has developed on what type of possible cyber war is, regardless of the fact that we have already faced one. Or third: we cannot observe the cyber military doctrine of the Serbian government for the following reasons:

- because we do not have an open and honest public conversation with key actors about the type of threats and possible scenarios for our cyber armed forces and the community facing moderate cyber warfare;
- because Serbia has not developed a defense doctrine for the cyber armed forces, with the support of the civilian sector, which would credibly play a relevant role in these scenarios;
- because there is no preventive diplomatic strategy to reduce the risk of such a war in Serbian diplomacy;
- because there is no articulated civilian defense strategy for the inevitable high impact of technological threats and the disruption of our civic economy in the community in the event of a possible cyber war;

- because there is no place in politics for the development of our IT industry base and workforce that can withstand all of the above to the extent that our national IT economy organizes technology support alliances.

Conclusion

Opponents or opponents will increasingly rely on technological means to carry out their operations, using cyber capabilities to control or support "hybrid operations." Hybrid warfare is not a classic military war that signifies armed conflict. Hybrid warfare is waged by unconventional means, primarily through the application of information technologies in, so to speak, the newly created space when we define it as cybernetic. This area has become very important for the work of security services in terms of defining possible threats coming from this area, but also in terms of conducting special psychological operations according to the identified goals, whether it is a state, community, people, vital infrastructure or even important individuals. Hybrid warfare is part of a special war, but the term refers to a specific action backed by a foreign intelligence service or services using modern means such as the Internet, social networks, portals, and specially designed sites in the cyber sphere. Cyber conflicts and cyber wars are great examples of the use of new technologies within hybrid threats.

LITERATURE

1. Laurence Ifrah, “States face new challenges from cyberwarfare and cybercrime”, Revue Défense Nationale, Vol. 714, 2008.
2. Thomas Rid, Peter McBurney, Cyber Weapons, The RUSI journal, Volume 157, 2012 - Issue 1
3. Joel Brenner, America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare, Penguin Press, 2011.
4. EastWest Institute, Annual Report 2020, https://www.eastwest.ngo/sites/default/files/ideas-files/ewi-2018-annual-report.pdf
5. Emerging Cyber Threats Report 2015, The Georgia Institute of Technology, https://www.cc.gatech.edu/sites/default/files/images/2015emergingcyberthreatsreport.pdf
6. Darko Trifunović, International Security and Asymmetric Threats, Asymmetry and Strategy, University of Defence Strategic Research Institute & National Defence School, Belgrade, Serbia, 2018
7. Franklin B. Miles, Asymmetric Warfare: An Historical Perspective, US Army College, Carlisle Barracks, Pennsylvania, 1999F
8. Paul B. Rich, Crisis in the Caucasus: Russia, Georgia and the West, Routledge, New York, NY, 2010
9. Carl Herberger, How to Defend Against Hacktivists, Information Security Media Group, 2013.
10. 8 Common Cyber Attack Vectors and How to Avoid Them, Balbix. https://www.balbix.com/insights/attack-vectors-and-breach-methods/
11. B. Todorović, D. Trifunović, Security Science as A Scientific Discipline - Technological Aspects, Security Science Journal, No. 1 (2020), Belgrade, Serbia, 2020. p.13 http://www.securityscience.edu.rs/index.php/journal-security-science/article/view/7/1

12. Greg Austin, Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security, Australian Center for Cyber Security, pp.19-20 https://www.unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/DISCUSSION%20PAPER%20Middle%20Powers%20REARMED%2027%20Jan%202016.pdf
13. The UK Cyber Security Strategy Protecting and promoting the UK in a digital world, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
14. 'Cyber Flag' Exercise Tests Mission Skills, From A U.S. Cyber Command News Release,US Dpt.of Defense, 2014. https://www.defense.gov/Explore/News/Article/Article/603637/