CYBER WARFARE: NEW TYPE OR WARFARE OR ADDITIONAL ELEMENT OF CONVENTIONAL WARFARE

Igor Novaković[*]
International and Security Affairs Centre – ISAC fund, Belgrade,
Republic of Serbia

Irina Rizmal[**]
Masters candidate at the University College of London,
Great Britain

Abstract: Cyber-attacks represent a new type of security threats, arising as a result of advancements in the field of information technologies, having the potential to change the dominant perception of conflicts. Since this threat is relatively new, and continues to evolve and change, it is difficult to foresee its future forms of development and potential manifestations of its use in conflicts. However, one should bear in mind that both the EU and NATO, as well as the USA, have already defined cyber space as a new military domain. The article discusses how conflicts are changing with the rise of this new domain, differing from conventional ones in both methods and means, and independent of norms of international law regarding the armed conflict/war. However, that does not mean that this new type of conflict is any less dangerous. Although belonging to the virtual sphere, cyber-attacks can leave considerable physical consequences. This article employs a comparative analysis of approaches to this topic, and then considers the perspectives of further developments in the cyber warfare, namely if there are possibilities for cyber to become a separate branch of war-waging, or, if it will remain only an additional element of conventional warfare, as it has already become with the advent of the so-called "hybrid warfare". This analysis represents a contribution to the discussion on the challenges of cyber in the future, providing a better insight into the potential challenges for our state in the present day and in the near future.

Key words: asymmetric threats, cyber space, cyber-attacks, cyber warfare, hybrid warfare

[*] Research Director, International and Security Affairs Centre – ISAC fund. E-mail: igor.novakovic@isac-fund.org.
[**] independent researcher and Masters candidate at the University College of London. E-mail: irina.rizmal@gmail.com.

INTRODUCTION

Over the past several years, cyber-attacks and cyber warfare became some of the most employed terms in debates on the future of conflicts and developing new approaches to security. Although in most countries decision-makers shaping modern international affairs increasingly place focus on "cyber" when it comes to security and defence policies, this field has not yet received enough attention in academic circles. In any case, cyber has been recognised by states as "the next big thing in security", seeing investment primarily in offensive cyber capabilities and the establishment of military cyber units for nearly two decades now. On the other hand, the academic literature has focused on debates over the efficiency of cyber-attacks and whether these pose a genuine threat as a new, completely independent form of warfare or not. In Serbia today, as is also the case when it comes to other asymmetric threats, this debate has been only somewhat opened, both in expert circles as well as in the public sphere.

The wider public in Serbia "became aware" of the challenges of cyber warfare with the outbreak of the crisis in Ukraine in 2014, with the advent of the term "hybrid warfare". This term is employed primarily by the "Western" media to describe Russia's engagement in the conflict in Ukraine, highlighting Russia's activities in the cyber sphere as one of its elements, focusing primarily the spread of disinformation as well as inflicting damage to strategic, viz, key infrastructure, critical for the functioning of the Ukrainian state. The North Atlantic Treaty Organisation (NATO) defines hybrid war as a blend of conventional and unconventional, regular and irregular, and information and cyber warfare.[405] Hybrid warfare, therefore, implies exploiting the full-spectrum (or some of its parts) of modern warfare and is not restricted solely to conventional means.[406] In this context, cyber warfare is understood as one option further complementing conventional warfare, enabling conflicts between states to also take place in the cyber sphere. However, the question arising is whether cyber warfare can exist as an independent form of warfare, autonomous from conventional forms? In this paper, we try to provide an answer whether there is a chance for such developments. The underlying hypothesis is that cyber-attacks will, in the near future, most likely remain a complimentary tool for conventional interstate conflicts, that is, that it will mainly be employed within the wider concept of hybrid warfare. Independent

---

[405] Van Puyvelde, Damien. Hybrid war – does it even exist?. NATO Review. http://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/ (accessed March 14, 2017).
[406] Ibid.

cyber-attacks will be present in smaller numbers, but will take place in controlled conditions, with the aim of the attacker to achieve a specific effect (panic, intimidation, deterrence, and the like), without the use of conventional forces. In order to test the hypothesis, we consider several approaches to the question of cyber warfare, primarily within the context of how they relate to conventional, Cold War forms of war-waging. For the purpose of this paper, focus is placed solely on cyber-attacks between states, directed towards information systems, networks and the information resident on them[407], which can be independent or feature as elements of an attack in which conventional methods are also employed.

DEFINING CYBER WARFARE

To date, only a limited number of authors attempted to explain the nature of cyber-attacks, with no clear conclusion on what the nature of these is to be like in the future.[408] From a historical perspective, every technological development produced new concepts that had become core for national security thinkers. After air power, nuclear and thermonuclear weapons, and the definition of space as a potential conflict domain, 'cyber' has become a new buzz word in security literature. Although the initial creators of the Internet, as a global network introducing cyber as a phenomenon, saw only the positive aspects in terms of networking and easier exchange of data, cyber also brought on a sheer volume of new security challenges and threats, among other, the threat of interstate conflict in the cyber sphere. There is general agreement that cyber-attacks pose a genuine threat to national security, branded as a state's "perfect strategic weapon", creating new ways of going to war.[409] A mere overview of changes in how leading world powers, as well as international political and security organisations, approach this field, suggests significant preparations for potential conflicts in this sphere are underway. Estimates show that over 140 nations are developing offensive cyber capabilities, while a

---

[407] Iasiello, Emilio. Are Cyber Weapons Effective Military Tools?*Military and Strategic Affairs* 7 no.1 (2015), 24

[408] SeeLibicki, Martin C. Cyber War as a Confidence Game,*Strategic Studies Quarterly*no. 5 (2011); Liff, Adam P. Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies* 35 no.3(2012); Rid, Thomas. Cyberwar and Peace.*Foreign Affairs* 92 no.6 (2013); Iasiello, Are Cyber Weapons Effective Military Tools?; Adams, John A. Jr. *Cyber Blackout:When the lights go out-Nation at Risk* (Friesen Press, 2015)

[409] See Geers, Kenneth. Sun Tzu and Cyber War (NATO Cooperative Cyber Defence Centre of Excellence, 2010); Libicki, Cyber War as a Confidence Game;Schmidt, Eric & Cohen, Jared. *The New Digital Age: Reshaping the Future of People, Nations and Business* (John Murray Publishers, 2013),Segal, Adam. *Cyber Blackout:When the lights go out-Nation at Risk*

significant number of countries are also building military cyber units.[410] The United Kingdom was the first country to officially confirm it is developing "a full spectrum military cyber capability, including strike capability"[411]. Clarke and Knake define cyber warfare as "unauthorized penetration by, on behalf of, or in support of, a government into another nation's computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, or falsify data, or cause the disruption of or damage to a computer, or network device, or the objects a computer system controls"[412].

It seems, however, that this definition is too wide, as not all conflicts between states can be considered as acts of war, warrying both in approach as well as intentions, intensity and, most certainly, consequences. In this sense, Singer and Friedman explain that, while drafting the UN Charter, things like "the interruption of postal, telegraphic, radio and other means of communications" were addressed and although considered as serious, were nevertheless not defined as an act of war.[413] Joseph Nye believes that only acts that have effects that "amplify or are equivalent to major kinetic (conventional) violence"[414] can be considered as acts of cyber war. Singer and Friedman believe there are two criteria deciding whether a specific attack can be considered an act of war. The first is whether the attack featured an appropriate level of force corresponding to conventional war, while the second is the existence of orientation and measurability, that is, the existence of a "directed and deliberate connection between causes and consequences". In other words, there needs to be a clear indication that a given attack is part of a wider approach of a given state aimed at compromising the functioning a target state's systems, including the security of its citizens, and that the amount of force used corresponds to that in conventional warfare.

However, even when fulfilled, it is questionable whether these criteria are enough for provisions of international law to come into force, as it is extremely challenging to apply these to conflicts in cyberspace. Starting with the Charter of the United Nations (UN) which sees interstate conflicts as violating territorial integrity and sovereignty of one state by another state or

---

[410] Iasiello,Are Cyber Weapons Effective Military Tools? 54

[411] Statement of the UK Defence Minister Philip Hammond, New cyber reserve unit created. UK Ministry of Defence. https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit (приступљено 25. мај 2017).

[412] Clarke, Richard A. &Knake, Robert K.*Cyber War. The Next Threat to National Security and What to Do About It,* (Harper Collins e books, 2010) 109

[413] Singer, Peter W. & Friedman, Allan. *Cybersecurity and Cyberwar. What everyone needs to know,* (Oxford University Press, 2014) 124.

[414] Nye, Joseph S. Jr, Nuclear Lessons for Cybersecurity. *Strategic Studies Quarterly* 5 no.4 (2011) 21.

groups of states, in the case of conflict in cyberspace we are immediately faced with the problem of this definition's applicability. Cyber conflicts do not necessarily imply the use of physical force, nor do they inevitably take place in a specific geographical space (although they can leave consequences).[415] Some authors define different instances when cyber-attacks can be defined as an act of war, that is, when international law can be applied. Most notable is the "Tallinn Manual on the International Law Applicable to Cyber Warfare", put together by international law experts of the NATO Cooperative Cyber Defence Centre of Excellence following the famous cyber-attack on Estonia in 2007.

However, despite the existence of such a document, there is a lack of will at the international level to accept the principles it suggests. It is important to note that cyber is still a new field in which states are still experimenting and exploring new capacities and opportunities it opens, especially in the offensive domain, posing thus as the "new gunpowder" of the twenty-first century.[416]States do not want to share information about their capacities and activities in the cyber sphere, which is why it is extremely difficult to mobilise political will at the international level to significantly regulate the use of cyberspace, at least in the near future. On the other hand, some states, like Russia, actively advocate for international regulation of cyberspace, that is, conclusion of new agreements regulating activities within this sphere, while, according to Clarke and Knake, the United States of America (USA) are the main opposition of such a process.[417] As long as cyberspace remains unregulated, it will be difficult to define specific types of cyber-attacks in international relations carried out independently, without the use of other methods of war-waging – as concrete attempts of cyber warfare.

CYBER WARFARE IN RELATION TO CONVENTIONAL CONFLICTS IN THE COLD WAR ERA

The greatest challenge for analysing the phenomenon of cyber warfare is the fact that examples of attacks carried out against states in the cyber domain have been relatively rare to date. Most conscientious are the following: attacks against governmental websites and financial institutions in Estonia in 2007; Israeli attack on Syrian air defence systems, that is, the military air

---

[415] Singer & Friedman,*Cybersecurity and Cyberwar. What everyone needs to know* 124

[416] Peter Round, director of capability, armament and technology at the European Defence Agency, cited in Cyber security directive held up in face of "Wild West". Euractiv. https://www.euractiv.com/section/digital/news/cyber-security-directive-held-up-in-face-of-wild-west-internet/(accessed May 25, 2017)

[417] Clarke &Knake, *Cyber War:The Next Threat to National Security and What to Do About It* 106

traffic control the same year; Russian attack on governmental and media websites and financial institutions in Georgia in 2008; the allegedly American-Israeli attack on Iranian nuclear facilities through planting the "Stuxnet" worm in 2010; North Korean attacks on South Korea in 2009, 2011 and 2013 and the Russian attack on Ukrainian electric grids in 2015. This leaves us with relatively limited material for detailed analysis. The only possible way in which the nature of cyber warfare can be examined at present is thus to compare certain parameters of conventional warfare from the last period prior to the development of cyber weapons (tentatively, Cold War warfare), with the characteristics of known cyber-attacks characterised as instances of cyber war in the media. These parameters include: attribution or the potential to identify the attacker; signalling and deterrence; giving up on first use; and the length of conflict.

Attribution. Providing "evidence" that a state initiated an attack is still practically impossible to do with certainty, which leaves attribution, or the detection of the perpetrator of a cyber-attack, as an often complicated task. The attacker has at his disposal plenty of opportunities to "cover his tracks" on the network. Attacks are usually conducted over a network of computers controlled through a virus or worm, a so-called botnet network of devices (zombie network) commonly situated at a different territory from that of the attacker and "unaware"of participating in the attack. Furthermore, states are still developing capacities for cyber warfare in secrecy, and it is mainly in secrecy that they also carry out attacks on other states, making it difficult to determine who the attacker is, unless the state itself takes responsibility. To date, the majority of states suspected of carrying out cyber-attacks have denied taking part, and only detailed, digital "forensics" can provide limited indication and mainly circumstantial evidence. For example, during the cyber-attack on Estonia in April 2007, the surrounding context suggested the attack came from Russia. Namely, in February the same year a dispute broke out in Tallinn between radical Estonians and ethnic Russian over the preservation of a monument dedicated to the Soviet Army in the city's centre, culminating in late April 2007. The monument was not demolished, being dislocated instead, but the dispute caused serious tensions with Russia, who did not look favourably to such a revision of the past. During the crisis' culmination, internet websites of around a hundred of key institutions, organisations and public service provides in Estonia – one of the most networked countries in Europe and the world – were swamped with access requests to such an extent that some servers stopped working and shut down, that is, they were hit with a

Distributed Denial of Service (DDos) attack.[418] It was later determined that the attack involved over a million devices, the greatest DDoS attack ever seen until then. Estonia pleaded to NATO for help, whose experts tried to determine with whom the "infected devices" communicated during the course of the attack. "Digital forensics" determined that the central computer managing the botnet network was located in Russia and that the programme code was written on a "Cyrillic keyboard".[419] Although the Estonian government publicly claimed Russia was behind the attack at the very outset, and despite experts concluding that the epicentre of the attack was in Russia, there have been no direct consequences, as "NATO's political leaders judged that the cyber-attacks were not an act of war"[420]. Moscow denied involvement in the attack on Estonia, while some government officials, after learning that experts had determined the attack originated in Russia, admitted it was possible that "patriotic-minded Russians, angered by Estonia's actions, had taken the matter into their own hands". This episode in itself shows how difficult it is to unequivocally determine responsibility in the case of a cyber-attack. What this also means is that, with the lack of attribution, retaliation outside of the cyber sphere is virtually impossible, as it is practically impossible to create the political conditions to label a country as the culprit for a given cyber-attack, not to mention interpreting the attack as an instance of cyber warfare.

Signalling and deterrence. When it comes to signalling and deterence, possibilities for states are limited due to several obvious obstacles for successful application of such approaches in a way made possible with conventional and nuclear weapons during the Cold War. The first obstacle is certainly the fact that the process of capacity development for waging wars in cyberspace is carried out in secrecy in most cases. The second is the fact that in the case of cyber-attacks, there is no awareness of how potentially dangerous such attacks are, that is, there is still no "demonstration effect" as was the case with nuclear weapons and their use on Hiroshima and Nagasaki.[421] As citizens are mostly unaware of the dangers stemming from the cyber sphere, it is potentially difficult to use both signalling and deterrence, that is, it is difficult to convince publics that such a conflict would be

---

[418] Clarke&Knake, *Cyber War. The Next Threat to National Security and What to Do About It,*14
[419] Ibid.
[420] Singer& Friedman, *Cybersecurity and Cyberwar. What everyone needs to know* 122-123. However, a direct consequence was the creation of the previously mentioned "Tallinn Mannual" and, according to the authors, NATO's Public Diplomacy Division made a short film about this event titled "War in Cyberspace".
[421] Clarke &Knake, *Cyber War. The Next Threat to National Security and What to Do About It* 92

"expensive".[422] In effect, as public awareness on the risks and threats of potential future conflicts in the cyber sphere is low, public pressure on decision-makers, partly necessary for a successful strategy of deterrence, is still lacking. A third obstacle is the fact that cyber weapons can mainly be used only once, meaning the opponent can generally develop defences from such weapons following the first attack[423] by building up and updating their own systems (and also share these with others). Therefore, states are reluctant to use the most sophisticated and possibly most dangerous cyber weapons they own, which could, in case of full-blown war, combined with conventional tools, potentially bring an advantage. The fourth obstacle is the fact that in the case of cyber weapons it is difficult to even predict the effect these could achieve in a potential conflict (which is a crucial aspect of communication for signalling and deterrence), for two reasons. First is the matter of what sort of defensive, that is, offensive capacities the state which is a potential target has at its disposal, whether it is defensively strong enough to deter or reduce the strength of the attack, and to what extent can its offensive capacities inflict damage on the attacker during a potential counter-attack. Capacity development in the cyber sphere opens unexpected new opportunities for smaller states, too, as a relatively cheaper and more accessible source of relative power compared to conventional types of attack. This enables militarily less developed states to develop capacities to inflict significant damage upon larger states. As a result of all factors listed, attacks in the cyber sphere are (still) mainly of lower intensity (and if directed against states, it is primarily to do with retaliation for political decisions and moves in the physical world), while states rather prepare the ground and "sow" weapons that can, potentially, be used in the case of "a more serious conflict". The second reason is the fact that one country's defences are not dependent solely on the creation of domestic defence capacities, but also on the "interconnectedness" of the state as such. In other words, unlike conventional weapons,the effects of which can be clearly predicted as these are generally equal everywhere (while the consequences certainly depend on the defence of those attacked and preparedness for the attack), in the case of cyber there is significant difference in the context of applicability of cyber-attacks on each state. The more a state is "interconnected", the greater the opportunity for a cyber-attack to have effects, and thus signalisation and deterrence make sense. Therefore, cyber warfare is, as a sophisticated branch of war-waging, best used

[422] Segal, *The Hacked World Order: How nations fight, trade, maneuver and manipulate in the digital age* 29
[423] Clarke &Knake, *Cyber War. The Next Threat to National Security and What to Do About It*94

against states that are largely "interconnected", that is, where the key systems – both military and civilian – are automated and dependent on management via networks. As a result, states with the greatest cyber capacities are also most likely to be targets, although these will, expectedly, also invest in cyber defence the most. The limited opportunities of using cyber warfare, solely on "interconnected" territories, significantly limits its use value as a potentially key or even a self-sufficient branch of warfare. Hence both signalling and deterrence also have quite a small use value, except when it comes to defence capacities.

In this sense, new trends have come to the fore lately, when it comes to signalling and deterrence, seeing representatives of states, instead of communicating the development of specific cyber weapons and the consequences these may bring, primarily focus on strengthening cyber defence capabilities. As US Deputy Secretary of Defence, William Lynn III, stated, "deterrence will necessarily be based more on denying any benefit to attackers than on imposing costs (for an attack) through retaliation"[424].

However, cyber-attacks can be used to deter opponents from activities in other domains, outside of the cyber sphere. An example of this is the allegedly American-Israeli "Stuxnet" worm attack in 2010 on Iranian uranium enrichment facilities, which were practically destroyed and a clear message to Iran to give up on this programme sent. The already mentioned Russian attack on Estonia can also be interpreted as a form of deterrence, not from an attack on Russia per se, but from disputes with the ethnic Russian population in Estonia. Such attacks, if successful, can send a strong enough signal to deter certain states from specific activities, although this is rather far from using strategies of signalling and deterrence in the case of cyber warfare as such.

First use of weapons. Finally, what cyber-attacks have brought about is the revisiting of the role of states as unitary actors. Despite international organisations such as the UN, EU, NATO and OSCE working on common responses to the challenges of cyber warfare, states are increasingly developing their own military cyber commands and investing in establishing their own, independent, offensive cyber capacity. In this sense, the development of the sphere and importance of cyber inverted traditional approaches to security towards an "each state for itself" framework. Instead of contemplating a Cold War-like 'No First Use Declaration', as we have seen, states are specifically focused on such first use in the cyber sphere, which may

[424] Cited in Segal, *The Hacked World Order: How nations fight, trade, maneuver and manipulate in the digital age* 83.

cripple the opponent and disable the systems that could otherwise be used to launch a counter-attack.

Time dimension and conflict. When it comes to the time dimension of conflicts, cyber conflicts and cyber wars cannot be seen in the context of classic conflicts where a clear line can be drawn between the state of war, or the duration of conflict, and peace. Each of the abovementioned attacks was only the peak of a series of activities most likely unfolding way before the conflict started, only to have the final manifestation taking place following contextualisation of the problem. That is, anticipating a problem in the future, states that carried out the cyber-attack, most likely penetrated "enemy systems" way before the manifestation phase, implanting viruses, worms and logic bombs. At the time of crisis outbreak, the time of actual use, these tools had been activated, or saw their effect increased to the maximum, in order to reach the desired effect. Therefore, cyber warfare actually enables the situation in which, in the words of Joel Brenner, former head of counterintelligence under the US Director of National Intelligence, we are "(…) in a constant state of conflict among nations that rarely gets to open warfare (…) and we have to get used to is that even countries like China, with which we are certainly not at war, are in intensive cyber conflict with us"[425]. Therefore, conflicts in cyber space constantly unfold and do not necessarily have negative implications for interstate relations at a given moment. Their real purpose (aside from intelligence activities and industrial espionage efforts) is to create the preconditions for the moment of conflict eruption, when the cyber sphere could be employed as one of the domains where the conflict would unfold and where there is a possibility that one side would have a key advantage.

HYBRID CONFLICTS AND CYBER WARFARE

The use of cyber weapons is far more visible and effective when employed in parallel with other kinetic, that is, conventional arms. In such cases, attacks in the cyber sphere are primarily used for disabling defence systems of both conventional and cyber defence in part or in their entirety, by spreading propaganda through attacks (which can be of various types) on websites of institutions and the media, intimidating civilian populations through the destruction or disabling of critical civilian infrastructure, and so on. In this sense, for example, the Israeli cyber-attack on Syria in 2007 was used for disabling air defence, as a result of which the air attack on

[425] Cited in Singer& Friedman, *Cybersecurity and Cyberwar. What everyone needs to know* 121.

installations was suspected to have been used for nuclear arms development that followed the next day encountered no resistance. In fact, it was completely unexpected.[426] Similarly, the Russian 2008 attack during the war in Georgia, launched simultaneously with the conventional conflict, had significant effects in terms of spreading propaganda and panic by attacking media and government websites. In both cases, cyber was a useful tool for one of the parties to the conflict, bringing about a desired outcome in both cases. The use itself was relatively painless, since neither government, due to ongoing conflict, had the need to conceal its actions. This means that cyber warfare will, in any case, almost certainly continue to manifest itself through hybrid conflicts.

CONCLUSION

As we have seen in this paper, interstate conflicts limited exclusively to the cyber sphere currently unfold in parallel with normal, everyday interstate relations. As a parallel dimension, cyber makes limited conflicts in the cyber sphere possible, while at the same time maintaining unhindered political and economic cooperation in the physical world. These do not grow into war, nor are they generally seen as such, because, in spite of generally reasonable doubt, it is extremely difficult to carry out attribution. Cyber weapons are generally not used for strategies of signalling and deterrence, primarily because states are unsure of their own strength, or that of their opponents in the cyber sphere, and most importantly, there is rarely awareness among the publics of opposing countries on the potential consequences of cyber-attacks and how serious these can be. However, it is clear that cyber-attacks will certainly remain an element upgrading conventional warfare, significantly complementing and increasing its effects, primarily related to civilian populations, but only to a limited extent. In other words, it is very unlikely that cyber will become a key or even a self-sufficient branch of warfare in the near future, but will primarily be used as a complementary force in ongoing conflicts. Even if attacks do take place, these will primarily be of a demonstrational character (signalling and deterrence) for limited, indirect goals.

However, if we look back, cyber, as a new form of international conflict, appeared on the scene only a little over a decade ago, coming fully into the spotlight in 2007. In such a short period, this potential form of conflict

[426] Clarke&Knake, *Cyber War. The Next Threat to National Security and What to Do About It* 10

has more than demonstrated its ability to become a far more serious testing ground for future wars than it is today.

LITERATURE

1. Adams John, A. Jr. Cyber Blackout: When the lights go out - Nation at Risk (Friesen Press, 2015).
2. Clarke, Richard A. and Knake, Robert K. Cyber War. The Next Threat to National Security and What to Do About It (HarperCollins e books, 2010).
3. "Cyber security directive held up in face of "Wild West" Internet". Euractiv.
4. https://www.euractiv.com/section/digital/news/cyber-security-directive-held-up-in-face-of-wild-west-internet/ (accessed May 25, 2017).
5. Geers, Kenneth. Sun Tzu and Cyber War (NATO Cooperative Cyber Defence Centre of Excellence, 2011).
6. Iasiello, Emilio. Are Cyber Weapons Effective Military Tools? Military and Strategic Affairs 7 no.1 (2015).
7. Libicki, Martin C. Cyber War as a Confidence Game. Strategic Studies Quarterly no. 5 (2011).
8. Liff, Adam P. Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. Journal of Strategic Studies 35 no.3 (2012).
9. "New cyber reserve unit created". UK Ministry of Defence (2013).
10. https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit (accessed May 25, 2017).
11. Nye, Joseph S. Jr. Nuclear Lessons for Cybersecurity. Strategic Studies Quarterly 5 no.4 (2011).
12. Rid, Thomas. Cyberwar and Peace. Foreign Affairs 92 no.6 (2013).
13. Schmidt, Eric and Cohen, Jared. The New Digital Age: Reshaping the future of people, nations and business (John Murray Publishers, 2013).
14. Segal, Adam. The Hacked World Order: How nations fight, trade, maneuver and manipulate in the digital age (Public Affairs, 2016).
15. Singer, Peter and Friedman, Allan. Cybersecurity and Cyberwar. What everyone needs to know (Oxford University Press, 2014).
16. Van Puyvelde, Damien. Hybrid war – does it even exist? NATO Review.
17. http://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/ (accessed March 14, 2017).

SAJBER RATOVANJE: NOVA VRSTA RATOVANJA ILI DODATNI ELEMENT KONVENCIONALNOM RATOVANJU

Igor Novaković[*]
Centar za međunarodne i bezbednosne poslove – ISAC fond,
Beograd, Srbija

Irina Rizmal[**]
student postdiplomskih studija na University College of London,
Velika Britanija

Apstrakt: Sajber napadi predstavljaju novu vrstu bezbednosne pretnje stvorenu napretkom na polju informacionih tehnologija, koja ima potencijal da preokrene dominantno shvatanje sukoba. Kako je pretnja relativno nova i ubrzano se razvija i menja, teško je predvideti forme njenog daljeg razvoja i potencijalne načine iskazivanja konfliktima. Međutim, treba imati u vidu da je već danas sajber prostor označen kao domen ratovanja od strane i Evropske unije i NATO, ali i od Sjedinjenih Američkih Država. U članku su razmotreni načini promene konflikata sa pojavom ovog novog domena, koji se razlikuju od standardnih po sredstvima i pristupima, i koji praktično ne zavise od međunarodno-pravnih normi koje se tiču oružanog sukoba, odnosno rata. Međutim, to ne znači da je ova vrsta sukoba manje opasna. Iako pripadaju virtuelnoj sferi, sajber napadi mogu da ostave znatne fizičke posledice. U članku je primenjena komparativna analiza dosadašnjih pristupa ovoj tematici, a potom su i razmotrene perspektive daljeg razvoja sajber ratovanja, odnosno da li postoje mogućnosti za dalji razvoj u pravcu posebne grane ratovanja ili će sukobi u sajber prostoru ostati samo dodatni element konvencionalnim vrstama ratovanja, kao što su već postali pojavom hibridnog rata. Ova analiza predstavlja prilog razmatranju prirode sajber izazova u budućnosti, i samim tim omogućava bolji uvid u potencijalne bezbednosne izazove za našu državu danas i bližoj budućnosti.

Ključne reči: asimetrične pretnje, sajber prostor, sajber napadi, sajber rat, hibridni rat.

[*] igor.novakovic@isac-fund.org.
[**] irina.rizmal@gmail.com