Hyper Threats to Critical Information Infrastructure: Bringing the AI in the Game

Metodi HADJI-JANEV
Military academy “General Mihailo Apostolski”, Skopje, University “Goce Delcev”, Shtip, Macedonia
Ira A. Fulton School of Engineering, Arizona State University, ASU, U.S.A.
metodi.hadzi-janev@ugd.edu.mk, hadzijanev@gmail.com

Abstract: Threats to critical infrastructure (CI) and critical information infrastructure (CII) gradually change in the contested security environment. In the age of power redistribution where states lose the monopoly of power, the ongoing digital transformation provides many benefits to improve the efficiency of CI and CII, but at the same time foster vulnerabilities. Both state and non-state actors exploit modern technologies in non-democratic ways to compensate for their disadvantage and compete with mightier perceived enemies. The article explains how emerging technologies led by artificial intelligence applications and systems are elevating the threats to CI and CII from asymmetric and hybrid to a whole new hyper level that requires greater attention by policy experts and lawmakers but also by security and defense professionals.

Keywords: Critical infrastructure protection, Artificial Intelligence, Asymmetric threats, Cyber Threats, Hybrid threats, Hyper threats

INTRODUCTION

The contemporary security environment is changing fast. The Cold War predictability is long gone and uncertainty dominates security analyses and assessments. Today, states no longer have a monopoly of power. In the new contested security environment state and nonstate actors acquire undemocratic methods and exploit modern technologies to achieve strategic ends, among others by threatening critical infrastructures (CI) and critical information infrastructures (CII). The ongoing process of digital transformation driven by the development of Information and communication technologies, artificial intelligence (AI) applications and systems (particularly in terms of machine learning and robotics) and quantum computing feed the growing paradox of our modernity. While these technologies improve the overall CI and CII efficiency and our way of life, the same technologies are a source of asymmetric, cyber and hybrid-based threats vectors.

The present article’s main argument is that AI applications and systems may elevate the asymmetric, cyber and hybrid-based threats to CI and CII to a whole new hyper threat level. To prove why this requires serious attention the article first explains how the security environment has changed and how the ongoing power redistribution reflects liberal democracies. Then the article explains how state and non-state actors are able to exploit modern technologies and provide asymmetric, cyber and hybrid threats. Finally, the article describes why AI applications and systems may cause hyper threats to CI and CII and why this requires urgent attention by the relevant stakeholders.

ON THE CHANGING SECURITY ENVIRONMENT

The International world order as we know it, stretched between the Westphalian concept of statehood and the UN system to regulate relations between the states and organizations that they have formed, is in crisis. The dominance of liberalism and its Western protagonists as victors after the end of the Cold War, the intensified processes of globalization, technological development and the ongoing digital transformation have, among others, spurred changes in the concept of security. These changes have affected how nations states as the subject of international law were able to utilize national instruments of power and provide security as an assumption to successful governance, societal functioning, and securing the overall national wellbeing. In short, these changes have instigated the process of power redistribution and erosion of the states' monopoly over power and at the same time raised the level of non-state actors. The problem with this transformative process is that the non-state actors are objects, not the subjects of international law and, therefore, there is a vacuum of accountability as a prerequisite for security.

These changes affect peoples' perceptions, values and expectations (how people behave, act and react; how they consume things; produce; how they reproduce; how they educate and live). In short, change is evident in diplomatic, political, and international relations contexts; in economic and wellbeing contexts; and, as a result of these, also in the security context (i.e., what we mean by being secured).

The dominance of liberalism after the Cold War has brought many changes that have eroded the state monopoly of power. The walls have disappeared, the market has expanded and all of these, initially, were seen as a positive change. However, it soon became clear that the flattening of the world (Friedman, 2005) would not bring to fruiting the most promising hopes of this change. Moreover, it became clear that international peace, the treaty-based order, expanding markets and as a result the extension and eventual consolidation of civil and political rights could not be taken for granted (Hawthorn, 1999). In short, people with different cultures, traditions, history, but also interests had and still have a different interpretation of what democratization and liberal democracy are. This is important because the unchallenged "Post-Cold War" liberalism had the ability to extend the liberal theory into the extreme practice and dominance of the core concern for liberalism that is individualism (Zacher & Matthew, 1995). Hence, the interpretation of the Social construct theory and the role of the state has experienced liberalistic denomination in translating it into practice. The ultraliberal idea resides in the assumption that the state is instrumental to the purposes of individuals. Individual influence on states and on security is mediated through groups and institutions within and across states. Individuals can create, sustain, and destroy institutions and thereby enhance or degrade national and international security (Doyle, 1997). Power redistribution has also become evident in economic terms.

Unchallenged liberalism and the hope for new prosperity have led to the rise and expression of self-ownership, also known as the sovereignty of the individual or individual sovereignty (Davidson & Rees-Mogg, 1999). Hence, the market extension that prizes self-ownership was, thus, seen as a logical enhancement of the spread of liberal democracy. The substantive conditions imposed by powerful entities such as IMF, European Central Bank or European Commission, are neo-liberal 'austerity' measures (e.g. privatization, liberalisation, labor market reforms, regressive tax increases) which were interpreted as necessary and imperative. As a result, these interventions in society have dismantled social contracts and disrupted existing social relations. Unfortunately, although there are many positive aspects of prizing sovereign individuals there are many residual effects that empowered authoritarian regimes to easily shortcut the distance of the two systems and create confusions and frustrations inside the liberal and democratic world. This power shift and its accumulation by individuals and groups could easily lead to chaos and disorder, and opportunities for disaster capitalism and super-elitism, that it may provide. (Beckett, 2018). Moreover, this shift, as some have asserted, led to the right-wing libertarians of Silicon Valley (Beckett, 2018) or has empowered authoritarian regimes to develop their own version of democracy and liberalism (Kagan, 2019).

This process has led to a reduction of states' power and an increase of the power and influence of individuals and corporation. Many of the largest corporations are mightier than many states. Even the most powerful states sometimes need to adjust their ambitions to match the corporate interests and goals. The private and public power of global giants like Google, Amazon, or Apple may best be described when Donald Trump met Apple chief executive Tim Cook to discuss how a trade war with China would affect Apple's interests (Khan, 2018).

The ongoing digital transformation enhances power redistribution. Emerging technologies such as information and communication technologies (ICT), artificial intelligence (AI) applications and systems (particularly in terms of machine learning and robotics), nanotechnology, space technology, biotechnology, quantum computing, etc. that drives the ongoing digital transformation affects the way individuals and groups across society live, work and interact. As a result, the advancement of these emerging technologies is conquering a range of fields across societies. While some of these connections and engagements have a pure economic goal, there are those with malicious intent that serve as a side-safe haven in other actors' political ambitions. Hence, while the promise of significant social and economic benefits, increased efficiency, and enhanced productivity across a host of sectors of the society are proudly recognized by the liberal leadership, the disruptive effects of these technologies are rather neglected. Technologies that enhance pluralism and democracy in the public sphere, bolster productivity, interconnectivity, and allow us to work in transnational teams also reframe our perception of security. Increasingly, the lines between Home Security and National Security, physical and digital space are blurred. All of these have unequivocally caused radical shifts in the security context as well.

The traditional understanding of national security has been gradually reconceptualized. National security usually was equalized with military threats beyond national borders. Thus, the acquisition, deployment and use of the military as an instrument of national power to accomplish national political objectives is a traditional way of considering security. Hence, the regulations (national and international), but also political and diplomatic concepts followed this logic and have developed certain patterns that were predominantly state-centric. The reconceptualization of the security, nevertheless, under the pressure of the power redistribution, is two-dimensional (Brown, 1994). First, there is a broadening dimension and second, there is a deepening dimension to this change. Today, security, among others, is shaped by non-military threats such as environmental scarcity and degradation, the spread of diseases, environmental changes, migrations etc., which represent the broadening change. The deepening change, on the other hand, refers to the considerations of individuals and groups, such as ethnic conflicts, civil wars and regime changes to support civil rights (pure libertarian domination) rather than focusing narrowly on external threats.

Therefore, the security threat today is not just seen as coming from outside the national borders, but also from attacking the critical infrastructures that drive the functioning of the states. Both state and non-state actors have understood that, in the evolving security realm, by employing the very changes and technological advancements, they can exploit critical infrastructures and pose asymmetric and hybrid threats to democratic societies.

ASYMMETRIC, CYBER AND HYBRID THREATS TO CRITICAL INFRASTRUCTURE - CI AND CRITICAL INFORMATION INFRASTRUCTURES – CII

The process of power redistribution from state to non-state actors and the rise of the corporate world among others have increased the importance and relevance of the critical infrastructures and critical information infrastructures. The most general definition of what constitutes CI or CII is that this is the infrastructure that represents the key systems, services and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security or any combination of those matters. The EU version of this definition was provided by the Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection (The Council Of The European Union, 2008). Accordingly, CII represent the ICT systems that are Critical Infrastructures for themselves or that are essential for the operation of Critical Infrastructures (telecommunications, computers/software, Internet, satellites, etc.) (ENISA, 2009). The question, nevertheless, is why and how the attacks on CII entail asymmetric and hybrid threats to national security.

Attacking CII is attractive because it poses an asymmetric advantage. Both non-state actors or states acting through proxies can attack from distance-remotely without exposing themselves. Furthermore, these attacks are at almost no cost compared to the effects and consequences that victims may suffer. As we explained above, the changes after the Cold War and the increased demands to support these changes have contributed to the creation of a network of networks of systems, services and infrastructures. These systems and services are highly interconnected and interdependent. They can move people, money, goods, services and information with higher velocity and volume. These systems and infrastructures are already present in the energy sector, transportation, communication, banking and finance sector, public health and safety, agriculture and food chains, but also include essential government services. Hence, the attack and the cascading effect are what make these attacks asymmetric and dangerous.

Another reason why asymmetry is of grave concern for the defender or protector of the CII is that attacking via the internet does not offer just anonymity but also reduces the ability of exposure and as a result revenge. Thanks to the technological advantage and technical infrastructures the internet still allows a certain amount of anonymity and action without being exposed. This is not just a problem of accountability but also of the ability to strike back and thus enforce some of the security concepts that have worked in the past. One example of such a concept that has secured peace and has discouraged potential attackers was deterrence and assurance of the consequences (Negeen, 2017). Non-state actors or the states acting through proxies were hesitant to use force or to attack fearing the consequences that arguably were allowed by the international law. The fact that cyberattacks on the CII can be camouflaged via very cost efficient and simple techniques is a serious problem for responsible governing authorities for two reasons. First, the legality of striking back. In this context, the law of self-defense (both in terms of customary international law and in terms of positive existing international law under Article 51 of the UN Charter) requires the responding authority to know the target and to structure a response to an armed attack in terms of necessity and proportionality (The United Nations, 1945). This puts the defender or protector in a burdensome situation because the cascading effects that attacks on the CII (due to interconnectivity and interdependence) can cause may be grave and unpredictable, possibly leading to total destruction or creating a situation where the defender/ protector may lose everything if he waits. The second problem arising from anonymity is with the legitimacy i.e. to ensure that the response is on the right attacker. Usually, as practice has shown, the attacks may come from multiple directions and the forensics had indicated that attacks originated from several states (that have nothing to do with the attackers' agenda).

Security experts have extensively argued that CII are soft targets, and therefore are attractive for non-state actors posing asymmetric threats. One of the reasons for this is that these systems and infrastructures (after the collapse of communism) were developed in a virtual security vacuum. This attitude has made them soft targets. In his book "Soft Targets", for example, Dean Ing, argued that:

"*The architects of these networks and infrastructures were mainly concerned with profit. In fact, cost reduction and efficiency were their highest priority. At the same time, the growing dependence on these networks had not been matched by a parallel focus on their security…* (Ing, 1996).

Similarly, Stephen Flynn argued that:

"…security considerations have been widely perceived as annoying speed bumps in achieving corporate goals …As a result the systems that underpin our prosperity are soft targets for those bent on challenging U.S. power.." (Flynn, 2004).

The high dependence on CIIs, their cross-border interconnectedness and interdependencies with other infrastructures, as well as the vulnerabilities and threats they face raise the need to address their security and resilience in a systemic perspective as the frontline of defense against failures and attacks (ETH, 2009). Many governments and security experts argued that the rise of the Internet as a key CII requires particular attention to its resilience and stability (The United States Presidential Policy Directive 21-PPD-21, 2013).

The Internet, thanks to its distributed, redundant design has proven to be a very robust infrastructure. As a result, CII protection – (CIIP) is driven by different policy drivers. These drivers straddle the boundaries of globalization, convergence and dependence, war, terrorism, cyber-attacks and natural disasters, up to law and regulations, directives and response plans.

Although these and some other concerns at various levels have urged enormous attention on CII protection elevating asymmetry to the concept of hybridity several years ago has raised the policy and security concerns to a whole new level. The term "hybrid threat" is not doctrinal or operational. It is more academic or came about through the attempts to explain how state and non-state actors are abusing modern technologies and are trying to pose new threat vectors through multiple domains (political, economic, military, civil, or information). Moreover, it refers to the attempts of state or non-state actors to undermine or harm a target by influencing its decision-making at the local, regional, state, or institutional level.

Unlike just asymmetric threats that may be sporadic without coordination, these actions are coordinated and synchronized and deliberately target democratic states' and institutions' vulnerabilities. They are conducted by using a wide range of means and designed to remain below the threshold of detection and attribution. Hence, CII or policies that drive them (as explained above) are just one segment to employ ambiguity. The ambiguity is thus created by exploiting the challenges to democracies stemming from the changes in the security environment (as described above and enhanced by intensified globalization, technological advancement, power redistribution and the rise of corporate actors). The escalating value crisis between the liberal democracies and authoritarian states (including the internal liberal crisis) erodes international norms and institutions and makes open Western societies targets of comprehensive hybrid action. The internal (liberal democratic) value crisis increases antagonization and divergence within and among long-term allies and increases their vulnerability to external interference. CII in this context is usually exploited as a powerful platform and force multiplier in the geostrategic competition.

The perpetrators are combining conventional and unconventional means – disinformation and interference in political debate or elections, critical infrastructure disturbances or attacks, cyber operations, different forms of criminal activities and, finally, an asymmetric use of military means and warfare. The complex asymmetric threats to CII are thus elevated to the new level and amplified with the actions that blur and exploit challenges in international and internal politics, at the edge between legal and illegal, and between peace and war thresholds (Hybrid COE, 2020).

Hence, the hybrid threats to CII contain the same challenges as asymmetric threats but are more complex and coordinated – the use of different proxy actors (patriotic hackers for example) to accomplish their strategic ends (Lokot, 2017). Hybrid action is cost-effective. They feed on the vulnerabilities of the target and use them against it. This makes hybrid action more difficult to prevent or respond to (Hadji-Janev, 2020). Nevertheless, the evolution of the threat to CII does not end here. There is a whole new hyper threat level introduced by the emerging technologies.

HYPER THREATS TO CRITICAL INFORMATION INFRASTRUCTURES

Emerging technologies such as information and communication technologies (ICT), artificial intelligence (AI) applications and systems (particularly in terms of machine learning and robotics), nanotechnology, space technology, biotechnology, quantum computing, etc. are driving the ongoing digital transformation. This process affects the way individuals and groups across society live, work and interact. Mounting concerns ranging from negative effects on labor force dislocations, including other market disruptions and exacerbated inequalities, to the new risks to public safety and national security dominate experts, academics and national security pundits' forums across the world. In the interconnected and interdependent world, the chances to isolate cascading effects and consequences of technological advances are minimal. The previous discussion on hybrid threats opens whole new channels of vulnerabilities against the Western liberal democracies, among others by exploiting CII. At the same time, however, according to a KPMG LLP (KPMG) and Forbes Insights tech risk management survey (very similar as Fynn and Ing argued before), an increased focus on emerging technologies to help transform businesses has not been matched by a parallel focus on the risks that come with their adoption (KPMG, 2017). Hence, as the report concluded, disruption became a new norm.

The dual-use nature of these technologies has already attracted crafters of the geopolitical interplay (Pant & Tirkey, 2019). On several occasions, NATO military leaders have concluded that modern technologies (more precisely AI) will profoundly change the warfighting and using the military as an instrument of national power in achieving strategic ends (NATO ATC, 2019). Addressing students in 2017, the Russian President Putin predicted that: “whichever country leads the way in AI research will come to dominate global affairs” (Vincent, 2017). China’s ambitions in this area are also clear: the country says it will become the world’s leader in AI by 2030 (The China State Council, 2017).

Some have even warned that the use of modern technologies in achieving strategic ends is driving the world to a “hyper war” (Allen & Husain, 2017). Disruptive technologies have already proved capable of affecting decision-making processes through the enormous speed of development and the ability of machine learning. NATO missions and operations, which involve a high number of different countries and military organizations, are already heavily dependent on data and information exchange. Adversarial employment of modern technologies could influence, and even alter, information and communication amongst NATO allies while an operation is ongoing, creating confusion and distrust (Valášek, 2017).

Today it is well accepted that applying AI systems in the security context brings an ability that is beyond just the asymmetric cyber capacities or hybridity. The asymmetry of these systems spans from their availability right up to the ethical, moral and legal boundaries of their applications. Terrorist organizations have so far proved creative and ready to employ whatever serves their cause (Heffelfinger, 2013). They would not be hesitant to employ AI systems and applications to achieve their strategic ends. Terrorists have proved keen on hacking and exploiting cyberspace to affect CII. Hacking these systems, overriding their algorithms and subordinating them to the terrorists’ goals is not impossible. Terrorists or hackers working in these capacities could endanger existing governments’ AI systems performing critical functions or missions. Moreover, AI can be effectively deployed to undermine trust among allies by discrediting their intelligence (Valášek, 2017).

States’ (or their proxies’) use of AI systems to expand intelligence, surveillance and reconnaissance capacities supersedes the gain of the asymmetric strategies, cyber espionage, and hybridity. AI systems and applications are able not only to collect but also to process massive amounts of data in a short time. By employing AI or hacking these applications and systems the intruders can compensate for the skill differential in manpower and thus elevate asymmetry to a whole new hyper level. In a world of mega data, IoT and multi-vector and multi-domain-based threats, fast decision-making is a priority.

AI systems can overcome the “cognitive burden” and avoid instinctive, emotional and rapid decision errors (Barton, 2019). Today, most of the CIP and CIIP plans, and procedures are based on the underlying assumption of the limitations of human capacities. These limitations could, for example, be in the context of:

- Manoeuvrability (to be in a different place in a short period of time),

- Mass (to overwhelm defenders' capacities in a short period of time);

- Economy (to act with surgical precision and cause collateral damage that could have negative consequences or additional logistical requirements in terms of replacement of forces after long engagement and stress etc.);

- Competency ("nerds" rarely have skills that require intensive and long physical training);

- Coordination – unity of efforts (to swarm the target or to cause the effect of an advanced persistent threat and overcome any redundancies with an ability to simultaneously disable cyber and physical defenses in a coordinated manner);

- Above all, AI can perform cognitively complex tasks on a continuous basis (making a decision under stress, after a long engagement with higher precision and without instant errors) (Walch, 2019)

AI thus affects two key important variables for CIP and CIIP: time and space. AI can transfer data, performance, and even behavior with greater velocity and with a higher volume. "Reinforcement learning" (an area of machine learning concerned with how software agents ought to take action in an environment in order to maximize the notion of cumulative reward) is already practiced in the gaming industry and is giving significant results in the autonomous automobile industry (Marr, 2018). Skills and knowledge (developed tactics, techniques and procedures) can be replicated in almost no time even remotely. The instant transfer learning capability cannot be compared with recruiting terrorists or developing a hackers' army. This requires time, and there are specific conditions that must be satisfied. Furthermore, collecting important data and adequately processing it could allow the opponent (state or non-state actors) to exploit vulnerabilities beyond predictable capacities. Amir Husain, founder and CEO of SparkCognition Inc., observed that "the advent of hyper war opens up the reinterpretation of our geostrategic future" (Ackerman, 2018). Hence, the ability to overcome the essential pre-requirements for CIP and CIIP by employing or corrupting AI systems and, at the same time, to cause asymmetric and hybrid threats via cyberspace, is raising the threat to a whole new "hyper" level.

CONCLUSIONS

Changes introduced after the Cold War by the dominance of liberal democracies, technological development and the ongoing digital transformation continue to infuse uncertainty and unpredictability.

The threats to national security today are not just seen as coming from outside the national border, but also from attacking the critical infrastructures that drive the functioning of the states. Both state and non-state actors have understood that abusing the very changes and technological advancement in the evolving security realm can exploit critical infrastructures and pose asymmetric and hybrid threats to democratic societies. Acting through proxies, the attacker can endanger democracies from a distance-remotely without exposing themselves. It is widely accepted that CI and CII are soft targets and that both state and non-state actors have learned how to employ asymmetry and challenge democracy in a hybrid manner. This means that challengers to democracies are combining conventional and unconventional means – disinformation and interference in political debate or elections, critical infrastructure disturbances or attacks, cyber operations, including different forms of criminal activities to compensate for their disadvantages and exploit weaknesses. Nevertheless, the attraction to use digital transformation in a geopolitical context raises recent concerns about the threat to CI and CII to a whole new level. Many authoritarian regimes and non-state actors are already competing to take advantage of the ongoing digital transformation which poses a new hyper threat to CI and CII. This unequivocally urges the policy and national security elites in the liberal democracies to seriously reconsider the protection of CI and CII.

REFERENCE LIST

Ackerman, K. R. (2018). “Hyperwar Is Coming Faster Than You Think”, Signal AFCEA, available at: <https://www.afcea.org/content/hyperwar-coming-faster-you-think>.

Allen, R. J. & Husain, A. (2017). “On Hyperwar”, Naval Institute, available at: <https://www.usni.org/magazines/proceedings/2017/july/hyperwar>.

Barton, T. (2019). AI offers the ability to reduce the cognitive burden on soldiers, video interview with Sarah Sicarrd, C4ISRNET, available at: <https://www.defencenews.com/video/2019/10/21/ai-offers-the-ability-to-reduce-the-cognitive-burden-on-soldiers/>.

Beckett, A. (2018). “How to explain Jacob Rees-Mogg? Start with his father's books”, The Guardian, available at: <https://www.theguardian.com/books/2018/nov/09/mystic-mogg-jacob-rees-mogg-willam-predicts-brexit-plans>.

Brown, S. (1994). “World Interests and Changing Dimensions of Security”, in Klare, M. & Chandrani, Y. (eds.), World Security: Challenges for a New Century, New York: St. Martin’s.

Davidson, D. J. & Rees-Mogg, W. (1999). The Sovereign Individual: Mastering the Transition to the Information Age, Touchstone.

Doyle, M. (1997). Ways of War and Peace: Realism, Liberalism, Socialism, New York: W.W. Norton.

ENISA (2009). Critical Information Infrastructures, available at <https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii>.

ETH (2009). CRN Report, Critical Infrastructure Protection, Center for Security Studies.

Flynn, S. (2004). America The Vulnerable How Our Government Is Failing to Protect Us from Terrorism, Harper Collins Publishers Inc.

Friedman, L. T. (2005). The World is Flat, p. x, Farrar, Straus and Giroux.

Hadji-Janev, M. (2020). “Hybrid Threats And International Law: Economy And The Use Of Force In Specific Context”, Contemporary Macedonian Defence, Vol. 19, No 37, pp. 21-31, available at: <http://www.mod.gov.mk/wp-content/uploads/2020/02/37-Sovremena-Makedonska-Odbrana-en.pdf>.

Hawthorn, G. (1999). “Liberalism since the Cold War: An Enemy to Itself?”, The Interregnum: Controversies in World Politics 1989-1999, Vol. 25, pp. 145-160, Cambridge University Press.

Heffelfinger, C. (2013). “The Risks Posed by Jihadist Hackers”, CTC Sentinel, Vol.6, Issue 7, available at: <https://ctc.usma.edu/the-risks-posed-by-jihadist-hackers/>.

Hybrid COE (2020). “Hybrid threats as a concept”, The European Center of Excellence for Countering Hybrid Threats, available at: <https://www.hybridcoe.fi/>.

Ing, D. (1996). Soft Targets: Terrorism in the American Heartland, Tor.

Kagan, R. (2019). “The strongmen strike back”, Washington Post, available at: <https://www.washingtonpost.com/news/opinions/wp/2019/03/14/feature/the-strongmen-strike-back/>.

Khan, S. (2018). Who is more powerful – states or corporations?, conversation available at: <https://theconversation.com/who-is-more-powerful-states-or-corporations-99616>.

KPMG (2017). Disruption is the New Norm. Forbes insight, available at: <https://advisory.kpmg.us/articles/2017/disruption-new-norm.html>.

Lokot, T. (2017). "Public Networked Discourses in the Ukraine-Russia Conflict: 'Patriotic Hackers' and Digital Populism", Irish Studies in International Affairs, Vol. 28.

Marr, B. (2018). "Artificial Intelligence: What Is Reinforcement Learning – A Simple Explanation & Practical Examples", Forbes, available at: <https://www.forbes.com/sites/bernardmarr/2018/09/28/artificial-intelligence-what-is-reinforcement-learning-a-simple-explanation-practical-examples/#f4f5fb4139ce>.

NATO ATC (2019). "Artificial Intelligence - A Game Changer for the Military", NATO Allied Command Transformation, available at: <https://www.act.nato.int/articles/artificial-intelligence-game-changer-military>.

Negeen, P. (2017). "Deterrence In Retreat: How The Cold War's Core Principle Fell Out Of Fashion", War on the Rocks, available at: <https://warontherocks.com/2017/12/deterrence-retreat-cold-wars-core-principle-fell-fashion/>.

Office of the Press Secretary (2013). Available at: <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resilience>.

Pant, V. H. & Tirkey, A. (2019), " Emerging technologies and geopolitical contestation", Observer Research Foundation, available at: <https://www.orfonline.org/expert-speak/emerging-technologies-and-geopolitical-contestation-50562/>.

The China State Council (2017). "Notice of the State Council on Issuing the Development Plan for the New Generation of Artificial Intelligence", State Development, No. 35, available at: <http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm>.

The European Union (2008). "Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection", Official Journal of the European Union, available at: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF>.

The United Nations (1945). The Charter of the United Nations and the Statute of the International Court of Justice, Art. 51, available at <https://treaties.un.org/doc/Publication/CTC/uncharter.pdf>.

The United States Presidential Policy Directive 21-PPD-21 (2013). The White House.

Valášek, T. (2017). "How Artificial Intelligence Could Disrupt Alliances", Carnegie Europe, available at: <https://carnegieeurope.eu/strategiceurope/72966>.

Vincent, J. (2017). "Putin says the nation that leads in AI 'will be the ruler of the world", The Verge, available at: <https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world>.

Walch, K. (2019). "Why Cognitive Technology May Be A Better Term Than Artificial Intelligence", Forbes, available at: <https://www.forbes.com/sites/cognitiveworld/2019/12/22/why-cognitive-technology-may-be-a-better-term-than-artificial-intelligence/#7c8cd006197c>.

Zacher, M. & Matthew, R. (1995). "Liberal International Theory: Common Threads, Divergent Strands", in Kegley, C. W. (ed.), Controversies in International Relations Theory: Realism and the Neoliberal Challenge, pp. 107–150, New York: St. Martin's Press.

Metodi HADJI-JANEV

Brigadier General, (Ph.D.), is an associate professor at the Military Academy General Mihailo Apostolski"-Skopje, a unit of University "Goce Delcev" in Stip, Macedonia and Adjunct Faculty Member at Ira A. Fulton School of Engineering, Arizona State University, ASU, U.S.A. His current scholarship focuses on legal aspects of countering asymmetric, cyber, and hybrid-based threats, with emphasis on critical information infrastructure and critical infrastructure protection; on legal and strategic aspects of use of force in countering terrorism and organized crime threats, and on development of legislation and strategic documents to effectively prevent and counter cyber and hybrid threat vectors.