Center for Cyber Security and
International Relations Studies

The Impact of Cyber Threat on Geopolitics:
A Paradigm Shift in International Relations

This paper aims to analyze the role and impact of cyber dimension on the traditional international relations' paradigms and theories. Since cyberspace is acting as a mother lode of conflicts, the new asymmetrical threats have deeply modified the traditional balances of power. Starting from the transforming effects of the informatization process and the new features resulted from the digital revolution, this work will analyze in details the geopolitical landscape. A particular focus will be on the current Middle Eastern scenario where continuous proliferation of cyber-weapons has shacked the fragile balance of Arab countries. To this end, the geopolitical tensions within the region will be further explored by detailing how the shift of the battlefield toward cyberspace has affected the political development in Iran and Qatar. Finally, the paper will provide an insight on the emerging future scenarios that are set to shape the international relations among States over the next few years.

Keywords: *Information Warfare, Cyber-Geopolitics, Stuxnet, Qatar-Gulf Crisis, APT*

Introduction

Over the last decade, the virtual component of the cyber dimension and the physical realm of the political sphere have kept interacting to the point they overlapped.
The *informatization* process has led to an inevitable shift of contrasts on the cybernetic sphere, which plays a pivotal role as it regulates the equilibrium of powers that characterizes the 21st century. Beyond land, sea, air and space, the cyber dimension represents the fifth domain of military and warlike activities, and it has gained a fundamental position. Across an increasingly liquid scenario, this process encompasses the use of transversal and asymmetrical threats that have deeply changed the traditional balance of international relations.

The history of cyber conflicts finds its roots in the ancient framework of military espionage and intelligence. Despite words as *Information Warfare* and *Cyber Threat* can be considered part of a modern lexical terminology, they are nothing more than an evolution – dictated by the contingency of the democratization of information – of the traditional concept of war. This new notion is then transliterated from the physical and psychological level to the virtual one, thanks to the militarization of the cybernetic space. As Jason Healey[1] points out, cyber conflicts' early signals can be traced back to the second half of the '80s, precisely in 1986 with the so-called Cuckoo's Egg case[2], when a computer security expert at Lawrence Berkeley Laboratory in the US discovered the intrusions of West German hackers. The event represented the very first case of espionage in the information age, since the hackers recruited by KGB managed to steal a large amount of highly sensitive information from the US systems, passing the data to the Soviets.

Although the paradigms of geopolitics and international relations are fundamentally the same, what has deeply changed is the scenario where such paradigms are grafted, due to the flexibility that characterizes the cyber domain. On this subject, taking into consideration the ancient military treatise "The Art of War"[3] attributed to the Chinese strategist Sun Tzu, it can be seen that, despite the aims are almost unaffected, both the arsenal of tools available to the threat actors and the victims' vulnerabilities have evolved dramatically. Such circumstances have caused a shift of the conflict's base to brand new paradigms, greatly different from those outlined in the Chinese treatise[4]. The new paradigms include first of all, the continuous improvement of tactics and tools, with constant updates and reconfigurations; secondly, the intangibility of the inner nature of cyberspace which makes the damages (or successes) measurement aleatory and uncertain; finally, the level of anonymity that characterizes actions carried on by state actors in the early stage of attacks. This anonymity makes the detection and the implementation of appropriate operation security practices complex, delaying emergency response mechanisms.

Interestingly, Gomez[5] describes the matter as a *techno-clash of civilizations* raising the issue of implementing a new model, in order to represent the asymmetry of the cybernetic panorama in the geopolitical field. At the same time, it is necessary to analyze the question through the concept of cyber-ubiquity: this approach implies that "every system in our technologically dependent civilization is a potential source of threat as the man made nature of the cyber domain places us all behind enemy lines"[6].

As Choucri[7] argues, the cyberspace features seven characteristics: temporality, physicality, permeation, fluidity, participation, attribution e accountability. Each of them contributes to replace the common understanding of the subject, consequently reshaping the social reality behind the international relations.

[1] Healey, J. (2013) *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.*

[2] Stoll, C. (2007) *The Cuckoo's Egg: Tracking A Spy Through The Maze Of Computer Espionage.*

[3] Tzu, S. (2003) *L'arte della guerra.*

[4] Geers, K. (2011) *Sun Tzu and Cyber War.*

[5] Gomez, R. (2014) *Cybergéopolitique: de l'utilité des cybermenaces.*

[6] Nieto, R. (2014) *Cyber-geopolitics. Geopolitical rivalries behind the cyber-threat narratives in the United States.*

[7] Choucri, N. (2012) *Cyberpolitics in International Relations.*

At a macroscopic level, the complexity of cybernetic sphere is reflected on the relations among Nations, whose concept of sovereignty goes beyond the traditional Westphalian notion. This generates a transnational model that uses brand new categories in order to delineate new (virtual and no longer linear) boundaries and features typical of the digital revolution. The traditional models lose their former meaning and acquire more undefined paradigms. In this way, usual concepts can no longer be applied to the conventional logic of conflicts. In fact, “victory and defeat are far from recognizable in cyberspace, as these concepts have little traction in a domain where political, ideological, religious, economic and military combatants fight for varying reasons according to different timescales. These actors bring their own code of conduct to the fight, resulting in a discordant and chaotic sphere of conflict in which it is not yet obvious that a common framework of ethics, norms and values can apply” [8].

Therefore, the old archetypes underlying international relations’ models and approaches need to be reconsidered in the light of the new interactions among all the involved players. According to Choucri[9], the conceptual frameworks behind the theories of IR – realism, institutionalism and constructivism – share the limit of focusing on static analysis rather than on transformational dynamics. This leads to the inclination of neglecting “the feedback effects or longer-term effects of short-term changes”[10].

The new model of international relations is now represented by an interconnected and anarchic system of continuously changing and developing interactions. It tends to eclipse the traditional state-centric approach that characterized last centuries’ stability.

The concepts of *power* and *supremacy* assume new meaning to fulfill the logic of digital space. The development of offensive capabilities in the cyber field does not follow the same path of conventional war arsenals. As Libicki points out, looking at the United States “given its conventional military power, the United States enjoys the kind of superiority that permits it to be the global cop, on the lookout for bad behavior without worrying terribly much about how others may react. This is not the situation in cyberspace”[11]. In fact, Washington’s military technological superiority does not make the country less vulnerable since “its society and, in particular, its military (with its attraction to network-centric warfare) depend heavily on information systems […] Thus, the United States, for all its advantages, might suffer more than adversaries would if retaliation begets counterretaliation”[12].

On this point and within the context of the cyber warfare, we can find three different information operation layers: physical, infrastructural and cognitive [13]. The physical layer is where the information overlaps with the physical world. The physical layer’s targets are computing and communication

[8] Cornish, P et al. (2010) *On Cyberwarfare*.
[9] Choucri, N. (2012) *Cyberpolitics in International Relations*. op. cit.
[10] Ibidem.
[11] Libicki, M. (2009) *Cyberdeterrence and cyberwar.*
[12] Ibidem.
[13] Ventre, D. (2012) *Cyber Conflict. Competing National Perspectives*.

systems, supporting infrastructures; In this case, cyber-attacks can be carried on through different methodologies ranging from cables' cutting to satellites' destruction. The second layer is the infrastructural one, representing the space where the information is collected, processed, disseminated and protected. Such attacks aim to jeopardize the information flow and they represent the core of the cyber warfare. Defacement, distributed denial of service, SQL injection, cross-site scripting are just a few examples of possible assaults conducted in the infrastructural layer. Finally, we have the cognitive layer that can be described as the space of the decision-making process relying on perceptions and awareness. The attacks to the cognitive layer have the strength to manipulate contents and consequently actors by spreading disinformation and altering the way the information is perceived[14].

The Digital Geopolitical Chessboard: Insight from Middle East

The transformation of the abovementioned theoretical paradigms comes with the ongoing process of creating new forms of law fitting the modern scenarios' complexity. This applies to *The Tallinn Manual on the International Law Applicable to Cyber Warfare* – version 2.0 released in 2017 – a project facilitated and led by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). The Tallinn Manual is designed as a reference tool for the application of the legal norms of international law to hostility cases in cyberspace. Starting from the rules on the applicability of *jus* and *bellum*, it aims to explore the concepts and principles of international law such as jurisdiction and sovereignty within the context of cyber operations in armed conflicts.

The need for effectively facing and regulating these issues arose strongly in the aftermath of the attacks hitting Estonia and Georgia in the mid-2000s. Such attacks showed clearly how the virtual and the concrete sphere were intertwined and interdependent. Indeed, the reasons behind the DDoS offensives launched by Moscow can be explained with its political agenda of those years aimed at extending and transposing the geopolitical tensions into the information warfare realm.

The causes of the attack to Estonia can be found in the tensions' exacerbation between the Baltic Republic and Moscow following the Estonian authorities' decision to remove the Bronze Soldier, a Soviet war statue dedicated to the memory of the Red Army soldiers who died in World War II. This led to mass protests across the streets of Tallinn and broke out into a full-on riot on April 26, 2007. Exacerbated by the Russian media, the clashes caused the imprisonment of nearly 1.000 people, while the number of wounded reached 150; moreover, the Baltic country IT infrastructures were stormed by an impressive cyber-attack.

[14] Ibidem.

Despite the requests of the Estonian authorities, the massive wave of attacks did not trigger NATO's article 5 on collective defense stating that any attack against one ally should be considered an act of war to all members of the Alliance.

The assault was carried on for almost a month through Distributed Denial of Service attacks, an orchestrated swarm of traffic that saturated the network by continuously exhausting bandwidth capacity. These actions' aim was to disrupt services and shut down the websites of several Estonian organizations such as banks and financial institutions, media outlet and broadcasters, universities and government entities.

The Georgian case is also paradigmatic as a clear example of hybrid warfare. In the summer of 2008, during the conflict in South Ossetia, Russia aimed to further weaken the Georgian government by combining kinetic and cyber-attacks. This set of actions is what has been defined as one of the first "implementation of measures for informational warfare in order to achieve political objectives"[15], such as the disruption of communications and the exfiltration of sensitive information. Defacement, DDoS, SQL injection, XSS and massive spamming on public email were some of the techniques used to hit the Georgian infrastructures, in parallel with the military operations related to the traditional war domain.

Thanks to this actions' synchronicity, the 2008 Russian-Georgian conflict has turned into a case study. From a tactical point of view, it is particularly interesting to note how some key-sites were targeted by cybernetic operations before the launch of military operations on a physical level. As pointed out by Kozlowski, among the targets of the Russian offensive there was not only the will to demonstrate the insubstantiality of Saakashvili regime – unable to react to the Russian assault –, but also the determination to cut the Georgian society off "from any information and present own propaganda in order to spread chaos and disinformation to undermine their morale and faith in government" [16].

Without any doubt, Russia's use of offensive cyber operations against Estonia (2007) and Georgia (2008) unveiled a brand new scenario. Nonetheless, the traditional paradigms of international relations and the axioms of geopolitics were revolutionized by the Stuxnet affair, a groundbreaking, imposing and complex cyber-attack against the industrial control system in Iran. In fact, Stuxnet's aim was not the disruption of the internet connection, neither the exfiltration of sensitive information. On the contrary, it was created to hit and infect a specific configuration in order to implement a genuine cyber sabotage against the industrial process control.

For sure, Stuxnet – together with its successors Flame and Duqu – represented the start of a new era of cyber threats, imposing a global afterthought about the impact of the cyber-dimension [and its reticular structure] on the physical realm. As a cyber-physical attack, it affected the three interacting

[15] Smith, D. (2014) *Russian Cyber Capabilities, Policy and Practice*.

[16] Kozlowski, A. (2014) *Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan.*

layers (IT, ICS, Physical) which make up the whole infrastructure[17]. The IT layer is exploited to propagate the malware; the industrial control system layer is used for the manipulation of process control; while the physical layer represents the structure where the damage actually takes place. In particular, "in the case of the cyber-attack against Natanz, the vulnerability on the physical layer was the fragility of the fast-spinning centrifuge rotors that was exploited by manipulations of process pressure and rotor speed" [18].

Analysts and researchers said Stuxnet represented a "game changer for malware defense"[19] and, in fact, the harbinger of a new form of warfare. As Tabansky argues, for the first time "a cyber-attack was chosen over available kinetic options and thrown into a battle of the highest strategic importance"[20]. Technically, Stuxnet was a malicious worm, spotted in 2010 but in development since 2005, infiltrating Teheran's facilities between June 22, 2009 and April 14, 2010[21]. It was deployed by Israel and USA in order to slow down the Iranian nuclear program as part of an intelligence operation named *Olympic Games*. Such operation was launched during George Bush's presidency and developed under Obama's administration with the aim of mapping Iran's sites and hinder Teheran's nuclear program.

Stuxnet represented a sophisticated threat targeting a specific Siemens software system. Designed with the aim of hitting the industrial control systems, it was able to self-replicate. Stuxnet could sabotage his targets by reprogramming the PLCs. It was able to deploy a wide range of tools to achieve its goals including rootkits, special evasion techniques and, above all, zero-day exploits. Stuxnet's destructive capabilities can be summarized by the Symantec malware analysts. Examining and describing the threat, they argued that "the real-world implications of Stuxnet are beyond any threat we have seen in the past. Despite the exciting challenge in reverse engineering Stuxnet and understanding its purpose, Stuxnet is the type of threat we hope not to see ever again"[22].

Showing a new warfare scenario, Stuxnet effectively represented a high-level technology weapon able to damage strategic objectives and critical infrastructures. In this regard, the malware capabilities required a reflection on the interdependent nature of the nation's infrastructure sectors. In fact, the risk – conceived as a function of threats taking advantage of vulnerabilities to damage or destroy assets – is summarized in the equation below:

$$\text{Risk (R)} = \text{Threat (T)} \times \text{Vulnerability (V)}$$

Due to the interdependence that characterizes it, the formula assumes an even stronger value in the

[17] Langner, R. (2013) *To Kill a Centrifuge.* The Langner Group, November 2013.
[18] Ibidem.
[19] Benson, P. (2010) *Computer virus Stuxnet a 'game changer' DHS official tells Senate*.
[20] Tabansky, L. (2016) op.cit.
[21] Falliere, N., Murchu, L. & Chien, E. (2011) *W32.Stuxnet Dossier*. p. 10.
[22] Ivi. p. 55

context of critical infrastructure.

The proven cooperation between USA and Israel in developing and spreading the threat has been part of the covert intelligence operation against Iran then developed through Flame, Duqu e Gauss. Stuxnet's dissemination undoubtedly marked a point of no return in international relations, particularly with reference to the balance of power in Middle East. In fact, following the events of Natanz, Iran "increasingly has contemplated cyberwarfare as a potential avenue of action against the West"[23].

Over the past five years, Iran's state-sponsored cyber groups have been constantly growing, also implementing more sophisticated techniques and undertaking technological developments. The Iranian government has steadily boosted its cyber arsenal in order to align and compete with the US and Israeli's cyber digital tools. Interestingly, such process has been conducted through the increasing politicization of the hacking community.

Illustrative examples include the *Shamoon* malware and the *Operation Saffron Rose* (2013-2014) led by the Iranian state-sponsored APT[24] *Ajax Security Team*. This group was responsible for different cyber espionage operations against defense companies in the US and political dissidents in Iran[25].

On the cybernetic level, the metamorphosis of the Iranian groups has reflected the volatile scenario characterizing the Middle East regional politics.

Within the geopolitical context, Iran is active across multiple battlefronts. For example, Iran and Israel have transposed their historical rivalry to the Syrian soil, deepening their involvement in the country and opening a new war front. Israel's objective in this regard is to tackle Teheran's efforts to take over Syria and fill the power vacuum after the demise of the Islamic State.

Moreover, last June Iran played a crucial role amidst the Qatar-Gulf dispute, one of the worst political and diplomatic crisis hitting the Middle East in the last few years. Interestingly, the crisis has revealed how the cyberspace is becoming the new domain for international relations, showing the impact of digital forces on the relations among States and recalling the attention on the need to enhance the efforts to regulate the cyber-attacks. At the end of May 2017, on the Qatar News Agency website appeared some statements attributed to the Emir of Qatar al-Thani in which he praised Iran, supported Hamas and accused Saudi Arabia. Despite al-Thani denied the facts, claiming the news agency had been hacked, Abu Dhabi and Riyadh charged Qatar as destabilizer of the Middle East. By planting "a seed of misinformation in a bed of long-standing tensions, a fake news story exploited regional polarization and anti-Iranian sentiments to rip the region further apart" [26].

[23] Berman, I. (2012) *The Iranian Cyber Threat to the U.S. Homeland*.

[24] The term stands for advanced persistent threats. APT groups work directly for the government, receiving orders and support from a nation state.

[25] Villeneuve, N., Moran, N., Haq, T. & Scott, M. (2013) *Operation Saffron Rose*.

[26] Kaush, K. (2017) *Cheap Havoc: How Cyber-Geopolitics Will Destabilize the Middle East*.

As a result, Qatar was cut off by its Arab neighbors (Saudi Arabia, the United Arab Emirates, Kuwait, Bahrain and Yemen) which broke all ties with the country accusing the Qatari Emirate to support Islamist terrorism and Iranian plans within the region. In fact, the reason behind Doha's isolation lies in the relations between Qatar and Iran, as shown by the 13-point list that Arab States issued to end the standoff and the Qatar-Gulf crisis. Among the requests, the coalition led by Saudi Arabia demanded to radically scale down any ties with Iran, cutting off diplomatic relations, military and economic cooperation, as well as expelling the members of the Revolutionary Guard. However, in contrast to Saudi Arabia's expectations, Doha's refusal to bend to those conditions strengthened Iranian regional presence and widened its jurisdiction and sphere of influence.

It is interesting to note how the Petro-Monarchies achieved the Qatar blockade through cyber tools and means. An action politically and diplomatically regrettable and unjustifiable was made possible thanks to the hacking of the QNA, permitting the Saudi coalition's move. A hacker group calling itself *Global Leaks* contributed to unveil the plan. The team released stolen emails from Yousef al-Otaiba, the United Arab Emirates ambassador to the United States, revealing both the UAE role in influencing US policy in Middle East and the cooperation with a pro-Israeli American think tank, Defense of Democracy (FDD). The messages showed a "clear collaboration between the FDD and the UAE on their joint efforts to cover the issue of Qatar and Kuwait of supporting terrorism. Other agendas included influencing Iran's internal situation using various political, economic, military and cyber tools"[27].

As we have seen, the Arab Nations' decision to isolate Qatar has been part of a greater plan, whose roots lie in the geopolitical dynamics of the Middle East, where political ambitions are intertwined with economic and strategic interests. In this regard, we can read Saudi King Abdullah bin Abd al-Aziz' words in a completely new light. As revealed by a WikiLeaks cable from 2008, King Abdullah urged US cooperation to overthrow Tehran regime from the inside with the aim "*to cut off the head of the snake*"[28].

Conclusion and Future Scenarios

The Middle East landscape shows how the continuous proliferation of cyber-weapons can shake and shape the fragile regional equilibria. Cyber-espionage, spywares and keyloggers, dissemination of propaganda and attacks to critical infrastructure are some of the new tools used by the States within the modern asymmetrical war scenario. This new kind of warfare has influenced not only the battle plans but also the basis of military strategy, adding a new level of complexity to the game.

[27] Bose, D. (2017*) Cyberwarfare in Qatar Crisis.*

[28] WikiLeaks Cable (2008) *Saudi King Abdullah and Senior Pinces on Saudi Policy Toward Iraq.*

In fact, the shift of the warfare toward cyberspace represents an obligatory and natural transition: wherever relevant activities blow up in the real world, akin operations fold out into the digital realm. This is why we refer to new paradigms with the term Geopolitics 2.0, "a new global reality which is characterized by three significant shifts: (1) states to individuals; (2) real-world to virtual mobilization and power; and (3) old media to new media"[29].

Within this framework, Choucri outlines four models, each of them representing a potential scenario related to the impact of cyber-politics in the international relations[30].

The first scenario, called *garrison cyber system*, refers to a world where country like North Korea, China and Saudi Arabia impose practices to control and deny Internet access incorporating cyber security in the sphere of national law and security. The second one, named *cyber anarchy*, predicts a future where conflicts and violence go hand in hand with the lack of governmental supervision; a kind of Hobbesian state of digital nature. A third model is represented by what Choucri calls *global cyber commons*: a world ruled by non-state actors marked by self-governance mechanisms where access to cyberspace is a human right. The last scenario is the *cyber grand bargain* with strong sovereign states able to undertake fruitful negotiations and collaborations. Such coordination will lead to several achievements related to the deployment of cyber tools to improve the human condition. Furthermore in the cyber grand bargain it is expected a "reduction in cyber threats and the growth of norms that support a viable cyberspace"[31].

Despite the differences amid the models, the changes caused by the cyber-revolution are already blatant and set to further develop over the next decade:

- Terrorist organizations make use of computer systems so much that the term cyber-terrorism has been coined. It refers to the intersection between terrorist activities and cybernetic reality and is "ideal for terrorists-as-communicators: it is decentralized, it is not subjected to control or restriction, it is not censored, and it allows access to anyone who wants it" [32].

- Governments, the Kremlin above all others, now routinely work to produce chaos and exploit cyberwar tools to spread disinformation through fake news and propaganda. It is what Basarab and Serdiuk call *hybression*[33] (crasis of hybrid and aggression) referring to Moscow's military strategy, designed to create havoc, polarize the society and paralyze the legal systems.

[29] Fraser, M. (2009) *Geopolitics 2.0.*

[30] Choucri, N. (2012) *Cyberpolitics in International Relations*. p. 233-238.

[31] Ibidem.

[32] Weimann, G. (2006) *Terror on the Internet: The New Arena, the New Challenges*. p. 25.

[33] Basarab, M. & Serdiuk, M. (2017) *The Kremlin's chaos strategy in Ukraine and its helpers.*

- Nation state-sponsored activities, and related APT groups, are increasing exponentially in the realm of cyber espionage. Supply chain attacks have become ever more sophisticated and difficult to mitigate. The reemergence of the *Shamoon*[34] attacks as well as the destructive diffusion of *WannaCry* and *NotPetya* are examples of this new States' engagement into cyber-warfare. In addition, the use of zero-day exploits and fileless infections is becoming an ordinary method to compromise networks worldwide. At the same time, as we keep on moving into a mobile environment, malwares impacting smartphones and mobile device are continually increasing. Not for nothing, governments have started to deploy powerful tools to compromise and monitor mobile phones in order to target journalists, human rights' activists and ethnic minorities with the aim of gathering confidential information.

Dealing with the asymmetric threat requires a confrontation with a new, broader and dual dimension where physical and cyber security's boundaries are blurred. This implies the need for a transformation – to be intended as adaption process – of the *security* and *defense* concepts[35]. Likewise, the global arena has assimilated the distinctive features of the cyberspace, such as uncertainty, fluidity and anarchy. This resulted in the shaping of constantly evolving processes, as the ones observed in the Middle East, especially the casus belli leading to the Qatar-Gulf crisis.

In this scenario, North Korea's situation represents a remarkable example. In fact, amid the efforts in developing nuclear weapons, North Korea's state-sponsored hackers have carried out some of the most daring cyber-attacks of the last few years, leading to the increase of Pyongyang asymmetrical advantage[36]. As a consequence, digital weapons have become a key asset of the North Korean arsenal as shown by the government-linked team *Guardians of Peace* operations' against Sony Entertainment[37] (November 2014), the *WannaCry*[38] ransomware outbreak (May 2017) and the *Lazarus Group*'s attacks to the SWIFT financial network worldwide. It has allowed North Korea to bypass the tough sanctions, generating an economic lifeline to fund the regime[39]. Indeed, because of the country's increasing isolation and fragile regional context, Pyongyang twofold purpose is to hit specific target's critical infrastructure as well as extorting money and manipulating online banking sessions to steal funds.

This is another demonstration of how the classic paradigms characterizing the international relations – both on a strategic and economic level – now respond to brand new logics encompassing information systems' architectures and cyber-physical interactions.

As a matter of fact, the digital side of geopolitics has managed to absorb the information revolution's

[34] Falcone, R. (2017) *Second wafe of Shamoon attacks identified*

[35] Ricci, S. (2017) *Cyber Warfare: Verso Un Nuovo Paradigma Strategico.*

[36] Siers, R. (2014) *North Korea: The Cyber Wild Card.*

[37] Haggard, S. & Lindsay J. (2015) *North Korea and the Sony Hack: Exporting Instability Through Cyberspace.*

[38] Sanger, D. (2017) *U.S. Accuses North Korea of Mounting WannaCry Cyberattack.*

[39] Wagstaff, J. & Smith, J. (2017) *Multi-stage cyber attacks net North Korea millions in virtual currencies: researchers.*

challenges. The rise of cyberspace as a *de facto* theater of battle and the absence of barriers enable actors to move their pawns on a fluid geopolitical chessboard where the balance of power evolves in conjunction with the fast-moving IT environment's changes. Undoubtedly, these new equilibria are set to be the driving force and the endogenous factors behind the emergence of upcoming political dynamics within the sphere of bilateral and multilateral relations.

Bibliography

Basarab, M. & Serdiuk, M. (2017) *The Kremlin's chaos strategy in Ukraine and its helpers*. Available from: http://euromaidanpress.com/2017/09/13/kremlin-chaos-tools-in-ukraine [Accessed 20th January 2018].

Benson, P. (2010) *Computer virus Stuxnet a 'game changer' DHS official tells Senate*. CNN, 17 November 2010. Available from: http://edition.cnn.com/2010/TECH/web/11/17/stuxnet.virus/index.html [Accessed 12th January 2018].

Berman, I. (2012) *The Iranian Cyber Threat to the U.S. Homeland*. (Statement), April 26 2012. Available from https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-071d.pdf [Accessed 13th January 2018].

Borg, S. (2012) *Logica della guerra cibernetica*. In: Limes, Quaderno Speciale, April 2012. pp. 47-53.

Bose, D. (2017*) Cyberwarfare in Qatar Crisis.* Centre for Land Warfare Studies, July 12, 2017. Available from: http://www.claws.in/1772/cyber-warfare-in-qatar-crisis-debashish-bose.html
html [Accessed 15th January 2018],

Buchanan, B. (2017) *The Cybersecurity Dilemma. Hacking, Trust and Fear Between Nations*. London, C. Hurst & Co. Publishers.

Choucri, N. (2012) *Cyberpolitics in International Relations*. Cambridge, MIT Press.

Cornish, P., Livingstone, D., Clemente, D. & Yorke, C. (2010) *On Cyberwarfare*. London, The Royal Institute of International Affairs, Chatham House. Available from: https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r1110_cyberwarfare.pdf [Accessed 14th January 2018].

Denning, D. (2012) *Stuxnet: What Has Changed?.* Available from: http://www.mdpi.com/1999-5903/4/3/672/htm#B3-futureinternet-04-00672 [Accessed 18th January 2018].

Falcone, R. (2017) *Second wafe of Shamoon attacks identified*. Available from: https://researchcenter.paloaltonetworks.com/2017/01/unit42-second-wave-shamoon-2-attacks-identified [Accessed 19th January 2018].

Falliere, N., Murchu, L. & Chien, E. (2011) *W32.Stuxnet Dossier*. Symantec Report. Available from: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf [Accessed 17 January 2018].

Fraser, M. (2009) *Geopolitics 2.0.* Real Instituto Elcano Report. Available from: http://biblioteca.ribei.org/1721/1/ARI-144-2009-I.pdf [Accessed 18th January 2018].

Geers, K. (2011) *Sun Tzu and Cyber War.* Available from: https://ccdcoe.org/sites/default/files/multimedia/pdf/Geers2011_SunTzuandCyberWar.pdf [Accessed 15th January 2018].

Giacomello, G. & Badialetti, G. (2009) *Manuale di studi strategici. Da Sun Tzu alle 'nuove guerre'.* Milano, Vita e Pensiero.

Gomez, R. (2014) Cybergéopolitique: de l'utilité des cybermenaces. *Cyberespace: enjeux géopolotique*. Hérodote, La Découverte, 2014/1, 98-122.

Haggard, S. & Lindsay J. (2015) *North Korea and the Sony Hack: Exporting Instability Through Cyberspace.* East West Center. Report number: 117.

Healey, J. (2013) *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Washington, Cyber Conflict Studies Association.

International Group of Experts at NATO CCDCOE (2017) *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, University Press.

Kaush, K. (2017) *Cheap Havoc: How Cyber-Geopolitics Will Destabilize the Middle East.* GMF, November 24, 2017. Available from: http://www.gmfus.org/publications/cheap-havoc-how-cyber-geopolitics-will-destabilize-middle-east [Accessed 13th January 2018].

Kozlowski, A. (2014) *Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan.* European Scientific Journal. Available from: http://www.eujournal.org/index.php/esj/article/viewFile/2941/2770 [Accessed 16th January 2018].

Langner, R. (2013) *To Kill a Centrifuge.* The Langner Group, November 2013. Available from: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf [Accessed 12th January 2018].

Libicki, M. (2009) *Cyberdeterrence and cyberwar.* RAND Corporation, Project Air Force.

Nieto, R. (2014) *Cyber-geopolitics. Geopolitical rivalries behind the cyber-threat narratives in the United States.* Available from: https://medium.com/homeland-security/cyber-geopolitics-a45fc698a3a1 pdf [Accessed 12th January 2018].

Ramo, J. (2009) *The Age of Unthinkable. Why the New World Disorder Constantly Surprises Us and What We Can Do about It*. Little, Brown and Company.

Ricci, S. (2017) *Cyber Warfare: Verso Un Nuovo Paradigma Strategico*. StreeLib, EPUB.

Sanger, D. (2017) *U.S. Accuses North Korea of Mounting WannaCry Cyberattack.* The New York Times, December 18 2017. Available from: https://www.nytimes.com/2017/12/18/us/politics/us-north-korea-wannacry-cyberattack.html [Accessed 13th January 2018].

Shane, P. & Hunker, J. (2013) *Cybersecurity: shared risks, shared responsibilities*. Durham, Carolina Academic Press.

Siers, R. (2014) *North Korea: The Cyber Wild Card*. In: Journal of Law and Cyber Warfare. 4 (1), 1-13.

Smith, D. (2014) *Russian Cyber Capabilities, Policy and Practice*. Available from: https://www.jewishpolicycenter.org/2013/12/31/russian-cyber-capabilities [Accessed 14th January 2018].

Stoll, C. (2007) *The Cuckoo's Egg: Tracking A Spy Through The Maze Of Computer Espionage*. New York, Doubleday.

Tabansky, L. (2016) *Cyber Power in the Changing Middle East*. Available from: http://turkishpolicy.com/article/804/cyber-power-in-the-changing-middle-east [Accessed 20th January 2018].

Tzu, S. (2003) *L'arte della guerra.* Milano, Mondadori.

Ventre, D. (2012) *Cyber Conflict. Competing National Perspectives*. London, ISTE Ltd.

Villeneuve, N., Moran, N., Haq, T. & Scott, M. (2013) *Operation Saffron Rose*. Available from: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf [Accessed 15th January 2018].

Wagstaff, J. & Smith, J (2017) *Multi-stage cyber attacks net North Korea millions in virtual currencies: researchers*. Available from https://www.reuters.com/article/us-southkorea-cyber-hackers/multi-stage-cyber-attacks-net-north-korea-millions-in-virtual-currencies-researchers-idUSKBN1ED0ZC [Accessed 19th January 2018].

Weimann, G. (2006) *Terror on the Internet: The New Arena, the New Challenges*. Washington, United States Institute of Peace.

Wikileaks Cable (2008) *Saudi King Abdullah and Senior Pinces on Saudi Policy Toward Iraq*. Cable: 08RIYADH649_a. Dated April 20, 2008 Available from: https://wikileaks.org/plusd/cables/08RIYADH649_a.html [Accessed 18th January 2018].

UNIVERSITÀ
DEGLI STUDI
FIRENZE

DSPS DIPARTIMENTO DI SCIENZE POLITICHE E SOCIALI
DISEI DIPARTIMENTO DI SCIENZE PER L'ECONOMIA E L'IMPRESA

Centro Interdipartimentale di
Studi Strategici, Internazionali e Imprenditoriali - CSSII

Tutti gli scritti pubblicati dal CSSII sono sotto la responsabilità esclusiva dei singoli autori