Militarization of Cyberspace, Changing Aspects of War in the 21st Century: The Case of Stuxnet against Iran

Saeid Reza Ameli

Professor of Communications and North American Studies, Faculty of World Studies & Faculty of Social Sciences, University of Tehran, Tehran, Iran,

Hassan Hosseini

Assistant Professor of North American Studies, Faculty of World Studies, University of Tehran, Tehran, Iran,

Farnaz Noori

PhD Candidate of American Studies, Faculty of World Studies, University of Tehran, Tehran, Iran,

Abstract

Militarization is perceived as the intentions of the military to intervene and overcome civilian procedures. The tendency for militarism generates from the military's ambition to be dominant over procedures not commonly perceived as military. It is described as an effort "to make people accept and love war, and see it as 'normal'" (Lutz, 2009a, in Bickford, 2015) and is usually associated with high military expenditures. On the other hand, the emergence of cyberspace has opened new capacities and paradigmatic frameworks for conceptualization of sociopolitical phenomena. The present article is concerned with the US use of Stuxnet against Iran's nuclear facilities in 2010. While being a cyber-tool in the US hostile foreign policy against Iran, the attack is discussed in the related literature as an act of cyber-war. This article argues that besides marking a cyber-tool in the US foreign policy against Iran, the attack was part of a long term militarization process in the US cyber strategy. Relying

on dual-spacization's assumptions of physical-virtual reality and using theory-testing process-tracing as the research method, this article concludes that the militarization process whereby Stuxnet was used as an alternative to kinetic attack on Iran, dual-spacized the nature of war.

Keywords: *dual-spacization, Stuxnet, militarization of cyberspace, process-tracing*

Received: 14/07/2020 Review: 13/09/2020 Accepted: 11/02/2021

Iranian Review of Foreign Affairs, Vol. 10, No. 1, Winter- Spring 2019, pp. 99-136

Introduction

The US use of Stuxnet against Iran's nuclear facilities is discussed in literature from different aspects. Debates vary on how Stuxnet marked the beginning of an era of changing the nature of war. They range from Liff's statement that Stuxnet was the "harbinger of what is to come" to Finkelstein and Govern's statements that cyberwar, as practiced by the Olympic Games[1], coined "a new label for the notion of war" which entails "not only a new kind of weapon, but an entirely new *genre* of war" [emphasis mine] (Govern, 2015: XIII).

According to Ben-Israel and Tabansky, in order for a cyber-attack to be identified as an act of war, several aspects of the action must be examined:

a. The organizational and geographical sources: whether a state is behind the action

b. Motive: whether it is possible to identify an ideological, political, economic, or religious motive for the attack.

c. Level of complexity: whether the attack required complex planning and coordinated resources that are available primarily to state agencies.

d. Results: whether the attack caused damage and casualties, and whether it would have caused damage without defensive actions were taken (Ben-Israel and Tabansky, 2014: 59-60).

The strategic definition of cyberwar by the US Department of Defense as "[t]he employment of cyber capabilities where the primary purpose is to achieve objectives through cyberspace …

1. the original name of the cyber-attack against Iran

[including] computer network operations and activities to operate and defend the Global Information Grid" (Vice Chairman of the Joint Chiefs of Staff, 2010, in Finkelstein and Govern, 2015: IX), is regarded by Finkelstein and Govern as bearing an implicit recognition in the concept of cyberwar being that "the US has a security interest" in electronic operations that eliminates the immediate impact of military operations on human life. "Protecting the Grid is comparable to protecting our physical borders" (Finkelstein and Govern, 2015: X). Given that Stuxnet was used as an alternative to physical attack on Iran's nuclear facilities, the military nature of the operation sounds the beginning of an era in which international conflicts extend to cyberspace as a strategic domain. The current article perceives the attack within the broader perspective of a longitudinal process within the US national security apparatus known as militarization of cyberspace, and argues that while reflecting the cyber dimension of the relationships, the attack can be regarded as having dual-spacized the nature of war in line with the US national security objectives.

I. Theoretical Framework

Dual-speciation is a new paradigm of understanding the capacity of new world order which looks at physical as well as virtual capacity of the world. Introduced in Saied Reza Ameli's [2003] article titled "Dual Globalizations and Global Risk Society", and later developed in his [2012] book, *Globalization Studies: Dual-Speciation's and Dual Globalizations,* Dual-Speciation refers to the existence of *virtual reality* beside *actual (physical) reality,* as a result of the emergence of cyberspace and globalization of communication. It stands upon the idea that as cyberspace has opened new capacities for conceptualization of social phenomena, a new paradigmatic framework has emerged for analysis in social sciences. The new framework is a dual-spatial one in which certain concepts bear a physical-virtual reality. Ameli (2012) distinguishes between the modern world and the globalized world, the former referring to the scientific developments achieved

during 18th, 19th and early 20th centuries and the latter refering to the period starting with globalization in different areas of communication, economy, society and politics. Then he explains how the *virtual world*, in parallel with the *real world*, has transactions and a geometrical reflection with it in all the globalized areas. He argues that the creation of the cyber world and its interconnection with the real world leads to a shift in our approaches and analysis trends of *the* new paradigm.

Ameli [2008] in Ameli, (2011) numerates the following characteristics for the physical world:

1. It world is defined and described geographically. We live within this geography and define *nearness* and *farness* based on it. Distances are measured by physical standards which determine concepts and definitions of political geography.

2. It is bounded to the *nation-state* system in the international structure. So, individuals are identified as citizens of nation-states, possessing specific civic rights under the jurisdiction of specific legal systems.

3. In the physical world, culture works as a social factor which enables the observer to distinguish between societies that are located in specific geographies and share common beliefs and lifestyles.

4. It is objective and can be felt by four senses. Things can be seen, smelled, heard and touched.

5. Communication takes place face to face and between present actors in the physical world, meaning that both sides have to be physically present for communication to be possible.

6. Time has a linear nature in the real world, meaning that the *past*, *present* and *future* appear in sequence and so things and events related to or happened in the past are further than things related to the present. So one can attribute *oldness* to certain things and *newness* to others.

The virtual world, on the other hand, depends upon the specific meta-factors explained below (Ameli, 2011):

1. Digitalization, the material of the second world is

numerical and it is indeed programmable based on algorithmic potential.

2. Dispersality, the distinction between center and periphery, near and far, disappears both in terms of geography and time. Based on such a potential, crowd-sourcing parallel to centralization of data and activation of data according to social algorithms would take place.

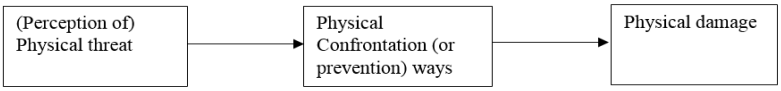
3. Borderlessness, cyberspace has no geography and its borders are not measurable by the physical world milestones, because 'place' has been replaced by 'space'. Users' presence, activities and sense of belonging, therefore, are not limited to borders of nation-states and their sovereignty.

4. Timelessness, virtual time is not a linear concept as it is in the physical world. The past, present and the future are present together. The 'cyber narration' flows in all these three times parallel to each other.

5. Comprehensive multiplicity, the network structure of cyberspace creates an unlimited communication complex in which effects, trends and phenomena are multiplied, aggravated and intensified with high speed and intensified with a network logic.

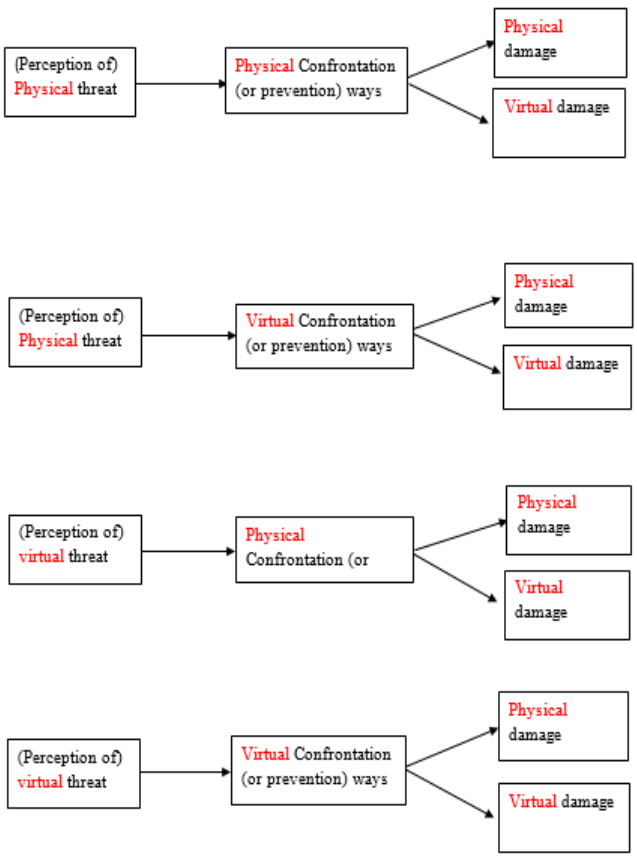
As a result of the existence of the virtual world parallel with the real world, the two spaces interact and affect one another. Thus, the analysis of many concepts in social sciences needs to be done within a new paradigmatic framework, a dual-spatial framework in which concepts bear a physical-virtual reality instead of their former physical reality. The idea of Dual-Specization of concepts and communications creates a basis for re-conceptualization and analysis of formerly defined notions in a physical/virtual framework. In this research, war is claimed to have gained a dual-spatial nature in Iran-US relations as part of the process of the US militarization of cyberspace. The idea is framed in conceptual terms as below:

Figure 1. War possibility in traditional wars



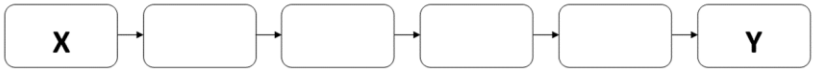
While in traditional wars, the threats perceived at any strategic moment, the confrontation ways adopted by strategy makers and the damages these confrontations left were all physical, in dual-spacized war either of the three can be physical-virtual, making a matrix of eight scenarios of how physical and cyber warfare can be used jointly and/or separately to attack or defend in a war.

Figure 1. Matrix of war possibilities in dual-spatial war



The research method used in this article to scrutinize the militarization process in which the nature of war is transformed into a dual-spatial one by the use of Stuxnet, is process-tracing. As a qualitative research method, process-tracing is "the analysis of evidence on processes, sequences, and conjunctures of events within a case for the purposes of either developing or testing hypotheses about causal mechanisms that might causally explain the case" (Bennett & Checkel, 2012: 10). George and Bennett (2005: 206, in Bennett & Checkel, 2012: 8) define process-tracing as the use of "histories, archival documents, interview transcripts, and other sources to see whether the causal process a theory hypothesizes or implies in a case is in fact evident in the sequence and values of the intervening variables in that case". In this method, the researcher starts from an outcome (Y) to trace the causal mechanism resulting in that outcome.

Figure 2. Causal mechanism in process tracing



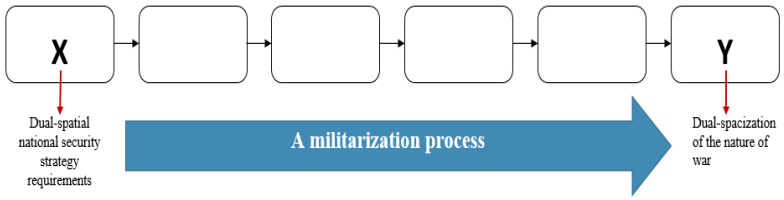
The key point for process-tracing is *causality*. Glennan (1992: 52, in Beach & Pederson, 2013, p. 1) defines a causal mechanism as "a complex system, which produces an outcome by the interaction of a number of parts".

In *theory-testing* process tracing, used in this research, the researcher hypothesizes that there is a causal relationship within a case (X contributes to producing Y). The causal mechanism between X and Y is *theoretically* supported. The objective of the researcher is to "opening up the black box of causality" to directly touch the details of the causal mechanism.

The hypothesis in this research assumes that there has been a military and strategic thinking in the US policy toward cyberspace, in that cyber-inclusive perceptions of threats, vulnerabilities, sources of power and the US role in the

international system shaped a vision of the US strategic environment in which the concept of security was extended to include cyber both as a source of threat and a capacity for national power enhancement. With the emergence of cyber as a domain with military, communicative and security functions, the United States had to found long-term military establishments in the new domain to use cyber power along with other instruments of power to exert influence worldwide. The expression of the perception is the institutionalization and development of cyber *offensive* operations to be used in line with other instruments of power. Development of cyber weapons to combat both physical and cyber targets indicates that first, militarization of cyberspace took place in line with national security requisites, and second, strategy making has been done dual-spatially. While defensive cyber operations had been part of the cyber strategy from a long time ago, offensive operations were tried to maintain national security in the *physical* world. The dual-spatial nature of war was marked by the launch of Stuxnet, i.e. the use of a malware (a *cyber*-weapon) to incur damage to *physical* infrastructures of an adversary. So Stuxnet contributed to dual-spacization of the nature of war as part of the longitudinal process of militarization of cyberspace.

Figure 4. Hypothetical process resulting in dual-speciation of the nature of war



II. Militarization of cyberspace

Schofield defines militarism as "the measure of the extent of use of military structures and procedures in a state's decision-making

process … the militarization of a state's decision-making process occurs when the military, or those possessing a military perspective, obtain relatively greater influence and the civilian policy-formulation institutions obtain relatively less influence" (Schofield, 2007: 11). According to Trauschweizer, militarism is associated both with "the military's predominance in foreign policy" and with "the employment of military force, rhetoric, and symbols in order to ensure elite control of the populace" (Trauschweizer, 2018). A more comprehensive definition is provided by Klare as "the tendency of a nation's *military apparatus* (which includes the armed forces and associated paramilitary, intelligence and bureaucratic agencies) to assume *ever-increasing control* over the lives and behavior of its citizens; and for *military goals* (preparation for war, acquisition of weaponry, development of military industries) and *military values* (centralization of authority, hierarchization, discipline and conformity, combativeness and xenophobia) increasingly to dominate national culture, education, the media, religion, politics and the economy at the expense of civilian institutions" (Klare, 1978: 121).

Olszewski believes that militarization of cyberspace results from "increasing saturation of the state structure with ICT technologies and the growing importance of these components in the process of ensuring security" (Olszewski, 2016: 104). According to Deibert, militarization of cyberspace refers to "the growing pressures on governments and their armed forces to develope the capacity to fight and win wars in this domain" (Deibert, 2011: 2). Gomez refers to three sets of criteria in literature to identify the militarization of cyberspace by states:

- A military doctrine or policy regarding cyberspace,
- A national cyber security strategy that recognizes state or state-sponsored cyber threats, and,
- A military and/or civilian unit(*s*) involved in to cyber defense and/or offense (Gomez, 2016: 48).

Using Klare's definition stated above, the trend observed as

militarization of cyberspace in this research covers the US cyber strategy to trace any policy decisions or practical initiatives that: *conveys the tendency or intention of the US military to have increasing control over procedures and mechanisms in cyberspace for military goals such as cyberwar or development of cyber warfare technologies and industries and military values such as centralization and hierarchization of US military authority in cyberspace;* It may include the engagement or the preparation of the state for a cyberwar and all its prerequisites: cyber warfare (weapons), cyber army (soldiers), etc.

Process tracing of the US militarization of cyberspace

The following sections scrutinize the US cyber strategy to indicate how the militarization process with the above definition is traced to prove the hypothesis.

Dual-spatial national security requirements

The emergence of cyberspace and its increasing role in international relations had implications for national security strategy making. The US has been the home country both to the cyber technology itself and the first discussions on cybersecurity as related to national security. But the inclusion of cybersecurity into the US national security agenda did not take place overnight. In fact, the link between *information technology* and *national security* was formed along with and as part of technological achievements in the military domain more than half century ago, when information infrastructures were regarded as military technological advancements. Hinsley and Stripp discuss the contribution and influence of Ultra[1] in the Second World War as a means for intelligence (Hinsley and Stripp, 2001). During the Cold War, information technology was regarded by the American military as a "force enabler" (Cavelty, 2007: 41) for emergency management, but the idea that it may be a serious source of vulnerability was first considered as late as 1980s when Ronald

1. the code-name used in the WWII for the decryption of enemy ciphers

Reagan was specifically concerned about the necessity of protecting 'classified information' (Cavelty, 2007: 44). Ever since, the issue of information threats to national security has appeared in the US national security documents.

At the outset of the new century, 9/11 attacks shocked America. The deadly bombings which happened on American soil and killed dozens of people, created uncertainties about the future security of the United Stated. The implication of the attacks for the US national security and foreign policy machinery was a change in perceptions of threats and security vulnerabilities of the country. The primary perception of vulnerability in the physical world after the attacks was so high that the prefix 'cyber' did not appear even once in the 2002 NSS document. Poulsen cites Marcus Sachs, the then white house office of cyberspace security saying:

> *We were shocked in the federal government that the attack didn't come from cyberspace [...]. Based on what we knew at the time, the most likely scenario was an attack from cyberspace, not airliners slamming into buildings [...]. We had spent a lot of time preparing for a cyber-attack, not a physical attack (Poulsen, 2003, in Cavelty, 2007: 103).*

The US cyber strategy in the early years following the attacks focused on enhancing federal computers' and IT infrastructures' security. In October 2001, George Bush issued an executive order 13231, "authorizing a protection program that consists of continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications and the physical assets that support such systems" (The National Strategy to Secure Cyberspace, 2003: 14) and in 2002, he requested that Congress increase funds to secure federal computers by 64 percent for the fiscal year 2003 (The National Strategy to Secure Cyberspace, 2003).

The first overarching document describing the US military's approach to cyberspace operations, was *The National Military*

Strategy for Cyberspace Operations, released by the Joint Chiefs of Staff in 2006. The document identified the role of the US armed forces as to ensure US superiority in cyberspace by conducting military operations. According to the strategy, the US would begin "integrating cyberspace operations with DOD's national defense role in the areas of military, intelligence, and business operations in the areas of military, intelligence, and business operations" (The National Military Strategy for Cyberspace Operations, 2006: 1).

The document recognized cyberspace as a foundation for Command and Control (C2) of military operations in other domains in need of unified action vertically and horizontally among all levels of war (The National Military Strategy for Cyberspace Operations, 2006: 11). It also asserted DOD's deterrence strategy to influence adversaries' decision making processes in collaboration with the intelligence community, law enforcement, counterintelligence, and other USG partners and allies (The National Military Strategy for Cyberspace Operations, 2006: 13).

This was followed by the 2007 Comprehensive National Cybersecurity Initiative (CNCI) which took a different approach. Linking the formerly separated cyber defensive missions with "law enforcement, intelligence, counterintelligence, and military capabilities to address the full spectrum of cyber threats from remote network intrusions and insider operations to supply chain vulnerabilities" (CNCI, 2007) was at the center of the strategy.

In Obama administrations, with relative success in the two wars in Iraq and Afghanistan, the physical threat from non-state groups and weak states to the US national security seemed to diminish though not disappeared. The first and the most important element of national interest, 'protecting the physical territory and the lives of Americans', which was endangered in 9/11, had been preserved. Therefore, when Obama took office in 2009, America faced a more diverse set of threats to national security. It was still suffering from economic crisis and fighting in the War on

Terrorism. The crisis had left the US economy with an increase in unemployment from about 4% in February 2007 to more than 7% in December 2008 (Escudreo, 2009: 28) and a decline in GDP at an annual rate of 6.3 percent in the fourth quarter of 2008 (Baily & Elliott, 2009: 4). Also, the US had spent $ 964.4 on the War on Terror between 2001 and 2008. While terrorism, violence and weak states constituted the main source of threat to the US national security in the two NSS documents published in 2002 and 2006, the NSS 2010 referred to terrorism as only one of the threats to the US national security: "terrorism is one of many threats that are more consequential in a global age" (NSS, 2010: 8). Extension of the sources of threat to national security made cyberspace appear in the list. The NSS 2010 recognized, for the first time, cyberspace as a source of threat to national security:

> *Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation. The very technologies that empower us to lead and create also empower those who would disrupt and destroy.*

The perceived threat in cyberspace was not solely coming from hackers and individuals but also from nation-states. Indeed, a substantial change in NSS 2010 to the 2002 and 2006 documents was that it extended characterization of the origin of *cyber* threats to the US national security from non-state actors and terrorists to state-sponsored activities: "The threats we face range from individual criminal hackers to organized criminal groups, from terrorist networks to advanced nation states" (NSS, 2010: 27). As other nation-states were developing their cyber military capabilities, they were perceived as sources of threat to the US national security via cyberspace. China and Russia were regarded as serious threats. "I can tell you that the Chinese have an aggressive goal to infiltrate all levels of U.S. government and private sector networks" said Dmitri Alperovitch, former McAffee cyber threat researcher, when asked about the consequences of a recent cyber-attack on the White House Military Office for

nuclear commands in 2012. Perception of threat to the US national security in cyberspace from China rose along with the observation of the Chinese "cyber jedis" (Hopkins, 2012) parallel to US engineers specializing in cyber intelligence. A report by the US-China Economic and Security Review Commission concluded in 2012 that "the Chinese People's Liberation Army (PLA) has long considered the ability to seize information dominance as prerequisite for achieving victory in future high tech conflicts, but only recently has it begun to develop the capability to convert this strategic requirement into an operational possibility" (Krekel et al, 2012: 14). The US-China Economic and Security Review Commission Reported to the Congress in 2012 that China was taking "a multipronged approach to the cyber domain" with "numerous stakeholders [who] influence cyber-related activities and priorities and a broad, national-level enterprise of government and military" (US-China Economic & Security Review Commission, 2012: 147) and that Chinese hackers, including state-sponsored actors, continue to "exploit U.S. information systems across government, industry, and civil society" (US-China Economic & Security Review Commission, 2012: 153). The report categorized Chinese harmful actors in cyberspace into four categories of military groups, intelligence and security services, independent actors and corporate actors. In another report prepared by Northrop Grumman Corp in 2012, Krekel et al stated that:

> *Earlier in the past decade, the PLA adopted a multi-layered approach to offensive information warfare that it calls Integrated Network Electronic Warfare or INEW strategy. Now, the PLA is moving toward information confrontation as a broader conceptualization that seeks to unite the various components of IW under a single warfare commander. The need to coordinate offensive and defensive missions more closely and ensure these missions are mutually supporting is driven by the recognition that*

> *IW must be closely integrated with PLA campaign objectives (Krekel et al, 2012: 8).*

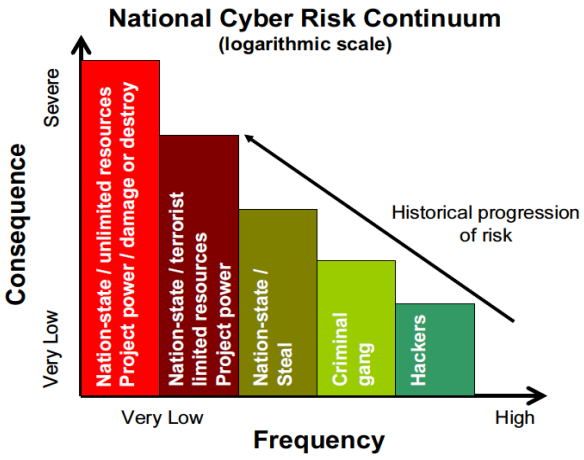
It was perceived that China was trying to integrate CNO1 with other types of information warfare such as electronic warfare, psychological operations, kinetic strike, and deception, and utilize them in a unified framework known as "information confrontation" (Krekel et al, 2012: 8). The US-China Economic and Security Review Commission warned that enjoying "538 million Internet users", China was developing "a pool of [cyber] soldiers" (US-China Economic & Security Review Commission, 2012: 149-152).

Beside China, Russia was also perceived as developing sophisticated advancements in the cyber domain. Moreover, Russia had a background of resorting to cyber-attacks in line with foreign policy objectives. It had attacked Georgia's communications network in 2008 due to a conflict between the two countries. Also, the 2007 DDoS attack to Estonia which disrupted the country from the net had been attributed to Russia. The Denial of Service attack to Estonia took place when Russia and Estonia were in dispute about the Estonian government's removal of a Soviet war memorial from Tallinn (Thomas, 2009). Though the Russian state denied any involvement in the attack, it was believed to have operated behind the event. As a result of the attack, "the country was literally wiped-out from the Internet" (Tofen et al, 2012: 103). It was assumed that a group of "patriotic hackers" in Russia, offended by Estonia's government decision, had committed the attack while receiving abet from the Russian state (Nye, 2010: 6). Also, the attack to Georgia happened in 2008 before Russian troops invaded the country. The impact of the attack was that it hindered Georgian elites from timely communication with each other and with the outside world (Sheldon, 2011: 104). The US ambassador to Russia, David Smith, noted that "Russia has integrated cyber operations into its military doctrine"; though "not fully successful … Russia's 2008 combined cyber and kinetic attack on Georgia was the first

practical test of this doctrine … [and] we must assume that the Russsian military has studies the lessons learned (Smith, 2012, in Cillofu et al, 2014: 12).

The emergence of other state actors with possible military power in cyberspace could threaten the US military superiority in cyberspace in that **first**, depending on the intension of the attacker, state-sponsored attacks are more probable to cause severe damage to critical infrastructures or steal sensitive information. As figure 5, published by the US Department of Homeland Security in 2009 shows, though the *frequency* of cyber-attacks to the US by nation states was lower than those committed by other actors, the *consequences* of such attacks, in case of happening, would be more severe.

Figure 5. The US National Cyber Risk Continuum (logarithmic scale).



Source: Cuts, 2009: 68

Second, longitudinal digitalization of basic infrastructures had made the US "a digital nation" (Cyberspace Policy Review, 2009: 13). The US critical infrastructure dependence on the cyber made it vulnerable to cyber threats. The dependence was expressed previously by Bush describing cyberspace as "the nervous system" of critical infrastructures and the "control system" (The

National Strategy to Secure cyberspace, 2003: vii) of the United States. Nearly all infrastructures in different sections of economy like agriculture, food, public health, government, information and telecommunications, energy, transportation, banking and finance depended on the Internet. Many military infrastructures of the US were also dependent on cyber. As Liff states, dependence on computers and networks and superiority can be paradoxically challenging for the US in that dependence on networks in both the military and civilian sectors, and the country's conventional military dominance, "paradoxically make it an inviting and vulnerable target for cyberattack" According to Liff, "The US military's growing dependence on commercial off-the-shelf products, many of which are made overseas, and the growing number of operational control systems (e.g., SCADA (Supervisory Control and Data Acquisition systems) and ICS (Industrial Control Systems)) that are connected to an IP (Internet Provider) network have made both military and civilian infrastructure increasingly vulnerable to cyberattack" (Liff, 2012: 409-410).

Third, the idea that the US power and influence should dominate in all areas including cyber, has persistently prevailed in the US strategic thought since the emergence of cyberspace. The preamble to the US constitution refers to "provid[ing] for the common defense, promot[ing] the general welfare, and secur[ing] the blessings of liberty" (US Constitution, 1788) as the three responsibilities for the American government. The Obama administration in both 2010 and 2015 strategies added a fourth objective: "[a]n *international order advanced by U.S. leadership* that promotes peace, security, and opportunity through stronger cooperation to meet global challenges" [emphasis mine] (NSS, 2010: 7). America's global leadership was a common issue mentioned in Obama administrations' NSS documents:

Our national security strategy is, therefore, focused on renewing American leadership so that we can more effectively advance our interests in the 21st century. We will do so by

building upon the sources of our strength at home, while shaping an international order that can meet the challenges of our time … Our approach begins with a commitment to build a stronger foundation for American leadership, because what takes place within our borders will determine our strength and influence beyond them. (NSS, 2010: 1-2)

The leading role for the US was explicitly mentioned in Hillary Clinton's remarks on the 2010 NSS, expressed on 27 May 2010: "Our approach is to build the diverse sources of American power at home and to shape the global system so that it is more conducive to meeting our overriding objectives: security, prosperity, the explanation and spread of our values, and a just and sustainable international order". The NSS 2015, too, insists that: "a strong consensus endures across our political spectrum that the question is not *whether* America will lead, but *how* we will lead into the future" (NSS, 2015: 2).

The assumption of the 'leading role for the world' was not void of a cyber-variable. Playing a leading role was compatible with the basic presupposition of the US position as the world's only superpower. Indeed, 'leading' the world would be impossible without comprehensive access to tools to exert power and influence. The new emerging domain for the exertion of power and influence is cyberspace. Maintaining 'a favorable order' in cyberspace, as an anarchic system with no stable governance and international ruling hierarchy, requires strong military presence and dominance. The new order may enjoy several characteristics but all in all it has to be in the US benefit, as the US International Strategy for Cyberspace read:

> *In the latter half of the 20th century, the United States helped forge a new post-war architecture of international economic and security cooperation. In the 21st century, we will work to realize this vision of a peaceful and reliable cyberspace in that same spirit of cooperation and collective responsibility (the US International Strategy for Cyberspace, 2011: 11).*

III. Cyberspace as a strategic domain for military dominance

The US strategic vision of the security environment included a military perception of 'cyberspace'. To combat threats in cyberspace and expand US power in the cyber world, cyber was regarded as a 'strategic domain' and a 'war fighting' front. As the first NSS document published under Obama, the 2010 National Security Strategy devoted special attention to cyber threats and mentioned cyberspace both as a source of vulnerability and military superiority for the United States:

> *Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation. The very technologies that empower us to lead and create also empower those who would disrupt and destroy. (NSS, 2010: 27).*

In 2010, the Quadrennial Defense Review called cyberspace "as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space", adopting a *strategic* view on cyberspace just as on the other four domains in which military operations are conducted (the Quadrennial Defense Review, 2010: 37). The approach was clearly reflected in defense strategy documents. The *National Military Strategy of the United States of America* stated that cyberspace has emerged as a war-fighting domain in its own right and that the US "will enhance deterrence in air, space, and cyberspace by possessing the capability to fight through a degraded environment and improving the US's ability to attribute and defeat attacks on systems or supporting infrastructure" (The National Military Strategy of the United States of America, 2011: 8). Also, DoD's *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* focused on the military goals in cyberspace such as defending networks and enhancing resiliency. The *Information Operations* (JP 3-13) of 2012 provided joint doctrine for the integration and coordination of information operations including planning, execution, and assessment programs across the range of military operations. The

Pentagon also provided the *Department of Defense Law of War Manual* (June 2015) including a chapter which clarifies DOD's interpretation of applicable law for conflicts in cyberspace. The *Cyber Electromagnetic Activities* (FM 3-38) of the US Army, published in 2014, included directions for conducting cyber electromagnetic activities and tactics and procedures for planning, integrating, and synchronizing them. The doctrine blends Army operations in cyberspace with electronic warfare and manipulating the electromagnetic spectrum.

The perception on the military nature of cyberspace for warfare operations was mixed with the intention to be the dominant military power in cyber. The assumption that strengthening cyber military capabilities for offensive operations could work as a means of *deterrence* in cyberspace, was the premise of Cold War strategic thought which prevailed in strategy making for cyberspace. The same logic seemed to be on stage regarding cyber threats. The US International Strategy for Cyberspace read:

> *The United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these vital national assets as necessary and appropriate (The US International Strategy for Cyberspace, 2011: 12).*

Development of cyber warfare was believed within the US security apparatus to be able to work as a tool for deterrence against both physical and cyber threats. The way for deterrence was to augment the costs of cyber-attack against the US:

> *We ensure that the risks associated with attacking or exploiting our networks vastly outweigh the potential benefits. We fully recognize that cyberspace activities can have effects extending beyond networks; such events may require responses in self-defense. (The US International Strategy for Cyberspace, 2011: 13).*

Based on the logic that "the best defense is a good offense" (Cilluffo et al, 2014: 20), the US was developing rules of engagement regarding cyber-attacks and cyber weapons. The efforts were designed to "recalibrate the defense to offense ratio" (Cartwright, 2012 in Cilluffo et al, 2014: 20) in favor of offense. Naming deterrence as "a subset of coercion" (Cilluffo et al, 2014: 18), a question for US policymakers to define a path forward was whether the US should engage in "the digital equivalent of an above-ground nuclear-test" as a deterring tool: "The ironic possibility that if conducted with care (commensurate to the enormity of the exercise) the cyber equivalent of such a test may be instrumental to deterring hostile actors and thereby preclude a fight is not to be dismissed out of hand" (Cilluffo et al, 2014: 19-20). What mattered in the deterrence discussion was that cyber operations were regarded as deterrent not only to cyber-attacks but to physical threats:

> *We will seek to encourage good actors and dissuade and deter those who threaten peace and stability through actions in cyberspace. We will do so with overlapping policies that combine national and international network resilience with vigilance and a range of credible response options (The US International Strategy for Cyberspace, 2011: 12).*

In line with this doctrine, the *Joint Cyberspace Operations* (JP 3-12) document, signed in February 2013, "addressed the uniqueness of military operations in cyberspace, clarified cyberspace operations-related command and operational interrelationships, and incorporated operational lessons learned" (Pernik et al, 2016: 14). The aggravation of attention to deterrence through offensive operations was intensified and more clearly expressed in the coming years. The *Quadrennial Homeland Security Review* of 2014 identified safeguarding and securing cyberspace as one of its five missions and called for "a secure and resilient cyberspace" (Quadrennial Homeland Security Review, 2014: 40). It assumed the responsibility of developing new and

expanded full-spectrum cyberspace capabilities and supporting military missions worldwide for DoD. According to DoD's Quadrennial Defense Review of 2014 the major roles of DoD in cyber include: "to defend the integrity of [DoD] networks, protect our key systems and networks, conduct effective cyber operations overseas when directed, and defend the Nation from an imminent, destructive cyber-attack on vital U.S. interests". While the 2015 *National Security Strategy* referred to the growing danger of disruptive and even destructive cyber-attacks, and called for increased investment in cyber capabilities, and "impose costs" (NSS, 2015: 13) on malicious cyber actors, DoD's *Cyber Strategy* of 2015 assumed the responsibility to be ready to conduct cyber operations to disrupt an adversary's military related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations", referring to DoD's offensive and operational capabilities.

While the DoD budget witnessed a decrease of $34.2 in 2013 and a decline in the overall funding for DoD budget and for federal government IT in 2015, funding for cyberspace operations increased by 8.5%. The increase was meant for the prioritization of R&D for cyberspace operations including defensive and offensive cyberspace operations and the development of USCYBERCOM's Cyber Mission Forces. In line with this change is an increase in national cyber security division budget from 346.5 million dollars in 2009 to 810 million dollars in 2014.

Institutionalization of cyber-military structures

A major trend identified as a step to militarization of cyberspace was stabilizing structural developments and establishments within the US state institution. Practical militarizing efforts took place in the department of defense (DOD) as the major government branch responsible for military activities. In less than a year after Obama took office, the US cyber command, known as USCYBERCOM, was added to the ten unified commands of the US department of defense on June 23, 2009. Defense secretary, Robert M. Gates nominated Lt. Gen. Keith Alexander, then director of the National

Security Agency, for a fourth star and to take on the top job at the CYBERCOM. While his nomination raised concerns among the Senate members about whether the new position could violate laws which prevent the military from operating in domestic issues, Alexander said to the Senate in his confirmation hearing:

> *This is not about efforts to militarize cyberspace; rather, it's about safeguarding the integrity of our military system. My goal if confirmed will be to significantly improve the way we defend ourselves in this domain. (Alexander, in Mount, 2010)*

The command is in charge of defending the US military's computer networks. The three headlines of the CYBERCOM mission include:

- Operate and aggressively defend the Department of Defense Information Network,
- Deliver cyberspace effects – both defensive and offensive – against global adversaries,
- Rapidly develop and deploy cyberspace capabilities to equip our force for the future fight against a resilient, adaptive adversary (US Army Cyber Command, 2020)

The operational roles and responsibilities of DOD in cyber security are conducted through USCYBERCOM Joint Operations Center, the National Security Agency/Central Security Service Center, the Defense Cyber Crime Center, and the Defense Information Systems Agency (DISA) (Pernik et al, 2016: 20). According to Deibert, the clearest example of militarization of cyberspace is the US Cyber Command "which unifies all of the existing military cyber activities under a single command". After the establishment of the CYBERCOM, the cyber components of all military services are to report to it. Its service elements include three-star commands representing each military service: Army Cyber Command (ARCYBER), US Fleet Cyber Command 10th Fleet (FCC/C10F), US Marine Corps Forces Cyberspace (MARFORCYBER), 24th Air Force (AFCYBER), and Coast Guard Cyber Command (CGCYBER) (USCYBERCOM Fact

Sheet, 2010) (Deibert, 2011: 2).

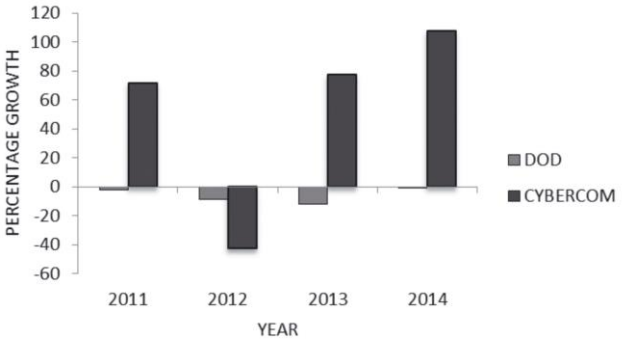
The establishment of the Command was highly controversial. There were concerns that "respect for privacy, diplomatic rules and sovereignty may be harmed as the administration accelerates its efforts to detect and attack adversaries on global computer networks that disregard borders" (Shanker, 2009). Also the "sheer size and importance of DOD's military operations" made some observers "wonder about how big an effect the Cyber Command might have outside its own domain" (Monroe, 2009). Controversies about the nomination made Bryan Whitman, a Pentagon spokesman, in discussing Gates's order say: "I can't reiterate enough that this is not about the militarization of cyber; this is an internal Department of Defense reorganization. It is focused only on military networks to better consolidate and streamline the department of defense capabilities into a single command" (Whitman, 2009, in Shanker, 2009).

While being responsible for centralized command and control of cyber operations, USCYBERCOM "leads day-to-day defense and protection of DOD information networks; coordinates DoD operations, provides support to military missions; directs the operations and defense of specified DoD information networks; and prepares to conduct full spectrum military cyberspace operations (USCYBERCOM Fact Sheet, 2009). According to Pomerleau (2017), an objective behind the construction of Cyber Command was for it to "act as an integrator and coordinator of cyber activities, namely offensive cyber activities, as to properly deconflict operations and prevent individual services from tripping over each other in cyberspace". While each service branch of the army has its own cybersecurity mission ranging from conducting electronic warfare to signal intelligence and information operations, USCYBERCOM ensures consistency among them (Pernik et al, 2016: 20).

Along with its establishment, budget allocation for the Cyber Command started and increased relatively as a share of the whole DOD budget. As figure 6 indicates, the percentage growth in the

CYBERCOM budget on an annual basis was much higher than the growth in the DOD budget itself.

Figure 6. Annual Growth in DoD and Cyber Command Budgets, 2011-2014



(Fung, 2014 & SIPRI, 2015 in Craig & Valeriano, 2016: 8)

The DoD also developed a Cyber Mission Force (CMF) in Obama second term to make up the Command focused on strategic and joint force commander problem sets. According to Pomerleau (2017), the CMF consists of 133 teams and 6,200 personnel including "13 National Mission Teams that defend the nation; 68 cyber protection teams that work to defend DoD networks; 27 combat mission teams that provide support to combatant commanders and generate effects in support of operational plans and contingencies, and; 25 support teams that provide analytic and planning support to the national mission teams". out of the 133 CMF teams, the Army provides 41, the Navy provides 40, the Air Force provides 39 and the Marine Corps provides 13 (Pomerleau, 2017). The 27 Combat Missions Teams support the combatant commands, such as the US Central Command, Pacific Command, and European Command. In November 2009, the Air Force announced that 27,000 communications officers were being transferred to provide support for cyber warfare operations from general computer communications, according to the *Air Force Times*. In April of this year, 3,000 more officers were moved,

bringing the total to 30,000.

Another program was the development of the National Cyber Range (NCR) as a DoD project originally established by the Defense Advanced Research Projects Agency (DARPA) and then under the supervision of the Test Resource Management Center (TRMC) to simulate cyberspace operations and test new technologies and capabilities. The objective is to test "throughout the program development life cycle using unique methods to assess resiliency to advanced cyberspace security threats" (Fergusen, et al, 2014). The NCR provides a "large-scale Global Information Grid (GIG) infrastructure, where technologies and systems can be analyzed and tested under real world conditions in current and future environments" (DARPA, 2008: 2).

Inauguration of the first cyber weapons for physical destruction

Whereas the US Air Force defines weapons as "devices designed to kill, injure, or disable people or to damage or destroy property" (US Department of the Air Force, 1993: 51-54 in Farwell & Rohozinski, 2011: 30), Liff states that cyber warfare are Computer Network Operations (CNO) whose means are non-kinetic and are committed with direct political/military objectives. CNOs fall in two categories of Computer Network Attacks (CNA) and Computer Network Defense (CND).

In practice, a serious and controversial example of the realization of the use of cyber warfare took place in 2010 under Obama namely operation 'Olympic Games' or malware Stuxnet as covered by media. Operation 'Olympic Games' was operated as an alternative to a kinetic attack on Iran's nuclear facilities. As the first "instance of a weaponized malware" (Gomez, 2016: 42), it is likened to the nuclear bombing of Hiroshima and Nagasaki by many security observers and practitioners including a former CIA Chief, Michael Hayden (Hayden, in Kaplan, 2016).

Stuxnet[1] harmed components of the Natanz uranium

1. "The name Stuxnet comes from a combination of file names found in the Stuxnet source code:.stub and MrxNet.sys" (Kosina, 2012: 76).

enrichment facility and destroyed over 1,000 centrifuges, marking "one of the first known uses of offensive cyber operations as a coercive measure between states" (Anderson & Sadjadpour, 2018: 9). The damage that Stuxnet brought about was comparable to a physical attack to Natanz. It infected over 60,000 computers, more than half of them in Iran; and the rest in other countries. It used four 'zero-day vulnerabilities[1], manipulated Siemens' default passwords and accessed windows operating systems that run the WinCC and PCS7 programs. Stuxnet infected Windows computers and looked for the Siemens SIMATIC WinC/Step7 controller software. If it did not find the Step7 software, it did nothing and incurred no harm. If it found the Step7 software, it infected the software in order to manipulate the PLC. The worm looked for high-frequency converter drives made by two manufacturers: Vacon (based in Finland) and Farao Paya (based in Iran). Zetter (2011, in Kosisna, 2012: 59) explains how it operated next: "after an initial period where it is dormant for two weeks, Stuxnet increases the frequency of the motors to 1,410Hz for 15 minutes. Then it restores the frequency back to normal (1,064Hz) and leaves it at this level for 27 days. After 27 days, it changes the frequency down to 2Hz for 50 minutes, then restores it again to 1,064Hz and waits for another 27 days before repeating the sequence. By interfering with the speed of the motors, Stuxnet thus sabotages the normal operation of the industrial control process". Besides incurring damage to the centrifuges, Stuxnet sent false data to the controller to assure them the systems were working properly and by disabling automated alarms misled scientists about what was actually happening in the site. The changes were highly specific, which indicates that Stuxnet

1. "Vulnerabilities previously unknown, so that there has been no time to develop and distribute patches" (Farwell & Rohozinski, 2011: 24). Zero-days are "the hacking world's most potent weapons" (Kosina, 2012: 60) because the vulnerabilities they exploit are neither known to the software maker not to the antivirus developers.

targeted a specific system and was planned to do its specific damage to the target.

IV. Dual-Spacization of the nature of war

Apart from the technical explanations about Stuxnet and other US-developed malware for offensive purposes, the use of the *weapon* marked a "revolution" in the history of military strategy. Farwell and Rohozinski believe that the attack marks a new era which has strategic "implications" and "lessons", being that "cyber-attack is not a distant theoretical probability" and that "cyber weapons may offer non-kinetic ways to disrupt an operational capability of an adversary". As mentioned before, the development of CNOs was perceived to contribute to cyber deterrence against both physical and cyber threats. Beside the actual damage it brought to the nuclear facilities in Natanz, the strategic implication "*Olympic Games* exemplified an operation intended to reduce the resistance of a rival system and to inflict attrition upon its resources. Destruction of an asset is one of many potential objectives that cyber weapons can achieve. Future cyber weapons may disrupt communications systems or the ability of adversaries to cohesively operate air, naval or ground forces. They could slow the speed at which an adversary is able to mass forces or deploy assets, destroying precious momentum vital for an adversary's offense" (Farwell & Rohozinski, 2012).

Stuxnet had all the features to be regarded as an act of war and realized the change formerly perceived in words not actions in the nature of war: *incurring actual physical damage by a computer virus developed by a nation-state to be used against an adversary*. The use of malware parallel with or instead of or an alternative to kinetic action. Within the framework used in this article, this is dual-spacization of the nature of war. The possibility of the replacement of a cyberwar for kinetic war has created an opportunity for a new generation of wars to come. According to Finkelstein and Govern, the change in the nature of war has occurred for three reasons: changes in offensive

capabilities, defense strategy and geopolitical change. They argue that:

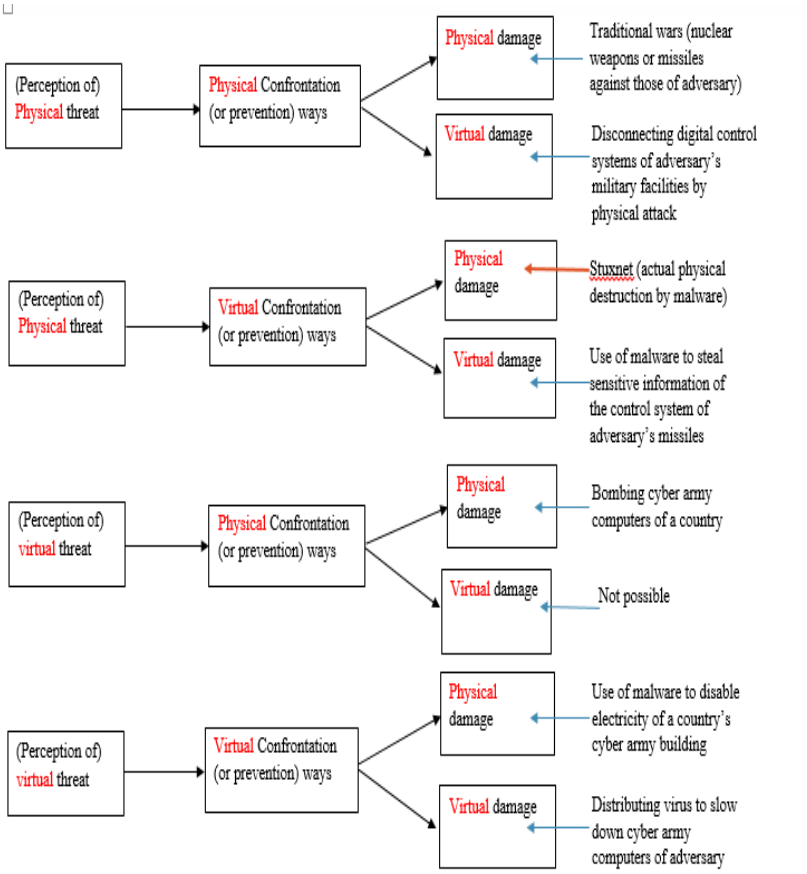
> *The possibility that we might be able to destroy a target like the Iranian nuclear reactor from the "inside out," avoiding detection for significant periods of time while an electronic virus works its way through the system's infrastructure, opens up the possibility of just such a dramatic change in our offensive capabilities. In addition, cyber technology creates the opportunity for a new kind of defense strategy, one designed both to counter cyber offensives and to pre-empt kinetic attacks, under scenarios that do not fit neatly within the traditional paradigm of war. When technological evolution is combined with geopolitical change, such as the demise of state sovereignty and the entrance of civilians or non-governmental actors into the arena of war, the transformative nature of cyber technology is enhanced (Finkelstein and Govern, 2015: XIII).*

Strategically, there are reasons for which cyberwar can be regarded as an alternative to kinetic war. The first one is that due to the nature of cyberspace, access to the infrastructures of the other side is possible without physical presence of the attacker. Ben-Israel and Tabansky state that this is a development happening for the first time in history. Besides is the issue of attribution (Ben-Israel and Tabansky, 2014: 61). Attribution after being attacked is a challenge in any war and the nature of cyberspace creates degrees of ambiguity on who has been behind the attack. Libicki states that ambiguity is the “unwillingness of states to say what they have done (or would do) coupled with the lack of proof that they have done it (or would do it)” and this is achieved in cyber: “The working hypothesis is that a cyber-attack used in lieu of kinetic methods creates more ambiguity in terms of effects sources, and motives” Libicki (Libicki, 2014: 43-46). One function of the attribution problem is that due to the specific

features of cyberspace, attacks could be launched by proxies (Liff, 2012: 413) making the attribution for the victim yet more complicated. From the legal perspective, the traditional Law of Armed Conflict requires that the victim identify the attacker to be able to launch a legal case; what can be difficulty achieved in the cyber world (Farwell & Rohozinski, 2011: 31). Stuxnet was a revealing example of the argument as for the substitution of Stuxnet, for military attack against Iran's nuclear program and how the United States preferred a cyber-attack over a military one to weaken or slow down some part of Iran's nuclear technologies. One asset, for instance, was that it did not cause the loss of life of Iranians; what was inevitable in case of a kinetic war. 'The costs' of cyberwar, in general, are less than those of a physical war.

Based on our conceptual framework, Stuxnet is to lie on the third line of our matrix: perception of *physical* threat from Iran's nuclear facilities provoked a *cyber* confrontational way with *physical* damage. Other types of dual-spatial war are also possible as figure 7 shows:

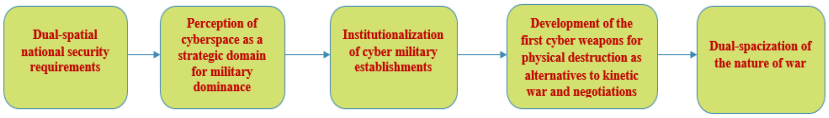
Figure 7. Types of dual-spatial war based on conceptual framework



The final process

Based on our hypothesis and experimental evidence, the final militarization process part of which was reflected in the form of Stuxnet looks as follows: dual-spatial national security requirements led to perception of cyberspace as a strategic domain for military dominance. Since military dominance needed long-term institutions responsible for its preservation, cyber military establishments were formed and the first cyber weapons were developed in them. The actual use of these weapons dual-spacized the nature of war. Figure 8 summarizes the whole process as below:

Figure 8. The process of the US militarization of cyberspace



Conclusion

The current article is focused on the US cyber-attack on Iran's nuclear facilities known as Stuxnet and argued that while giving a cyber dimension to the relations, the attack was part of a long-term militarization process in the US cyber strategy to dominate cyberspace a strategic domain. The central argument was developed as a hypothesis and tested through the means of the research method. Using dual-spacization as theoretical framework, the concept of cyberwar was conceptualized and the process of the US militarization of cyberspace was traced by process tracing as the research method. Findings prove the hypothesis in that dual-spatial national security priorities as to have military dominance in cyberspace contributed to the militarization of cyberspace through a chain of events starting from the necessity for a cyber-inclusive perception of national security requirements. Once cyberspace became a component of national security decision making, it was regarded as a domain for military dominance leading to development of *offensive* cyber operations with *physical* destructive impacts which in turn dual-spacized the nature of war. Stuxnet exemplified the use of a malware (a *cyber*-weapon) to incur damage to *physical* infrastructures of an adversary.

References

Ameli, S. R. (1382 [2003 A.D.]). Do fazāyi šodan-hā va jāme'e-ye jahāni-ye ezterāb [In English: Dual –Speciation and the Global Stress Community]. *Journal of Social Sciences Letter, 6*(21), pp. 143-174 (in Persian)

Ameli, S. R. (1390 [2011]). Ruykard-e do fazayi be āsib-hā, jarāyem, qavānin va siyāsaha-ye fazā-ye majāzi [In English: dual spatial approach to cyberspace harms, crimes, laws and policies]. Tehran: Amirkabir (in Persian)

Ameli, S. R. (1391 [2012 A.D.]). Motāle't-e jahāni šhodan: do fazāyi šodan-ha va do jahāni šodan-ha [In English: *Globalization Studies: Dual-Spacizations and Dual Globalizations*]. Tehran: Samt (in Persian)

Anderson, C. and Sadjadpour, K. (2018). *Iran's Cyber Threat Espionage, Sabotage, and Revenge*. Carnegie Endowment for International Peace. Retrieved form: https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf

Beach, D. and Pederson, R. B. (2013). *Process-Tracing Methods Foundations and Guidelines*. Michigan: the University of Michigan Press. Retrieved Jul. 24 from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=2ahUKEwiK2vuY_MzjAhWdD2MBHc1ZBaYQFjADegQIARAC&url=https%3A%2F%2Fedisciplinas.usp.br%2Fpluginfile.php%2F4250035%2Fmod_folder%2Fcontent%2F0%2FTextos%2FBeach%2520and%2520Pedersen%252C%2520Process-Tracing%2520Methods%2520-%2520Foundations%2520and%2520Guidelines.pdf%3Fforcedownload%3D1&usg=AOvVaw1Fl_oZU2yTJkN0MZ2kpNLB

Bennett, A. (2010). Process Tracing and Causal Inference. In H. Brady and D. Collier (Eds.), *Rethinking Social Inquiry* (2nd Ed.) (pp. 207-220.). UK: Rowman and Littlefield. Retrieved from: https://core.ac.uk/download/pdf/11923055.pdf.

Bennett, A. and Checkel, J. T. (2012, Jan). Process Tracing: From Philosophical Roots to Best Practices. Working Paper No. 21/2012. Vancouver: Simon Fraser University Simons Papers in Security and Development. Retrieved Jul, 24. 2019 from https://core.ac.uk/download/pdf/56379008.pdf

Ben-Israel, I and Tabansky, L. (2014). An Interdisciplinary Look at Security Challenges in the Information Age. In Siboni, G. (Ed.). *Cyberspace and National Security* Selected Articles II (pp. 51-67). Tel Aviv: INSS Institute for National Security

Studies Retrieved from:

Bickford, A. (2015). Militaries and Militarization, Anthropology of. Retrieved from Science Direct: https:// www. sciencedirect. com/ topics/ social- sciences/ militarization

Blueprint for a Secure Cyber Future. (2011). Department of Homeland Security. The Cybersecurity Strategy for the Homeland Security Enterprise. Retrieved form: https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf

Cavelty, M. D. (2007).Cyber-Security and Threat Politics: US efforts to secure the information age. EBOOK. Retrieved

Cilluffo, F. J.; Cardash, Sh. L. and Salmoiraghi, G. C. (2014). A Blueprint for Cyber Deterrence: Building Stability through Strength. In G. C. Siboni (Ed.), *Cyberspace and National Security (Selected Articles II*) (pp. 7-27). Tel Aviv: Institute for National Security Studies. Retrieved from: http://din-online.info/pdf/in2e.pdf

Craig, A. and Valeriano, B. (2016). Conceptualising Cyber Arms Races. Paper Presented in 8th International Conference on Cyber Conflict Cyber Power https:// www. researchgate. net/ publication/ 305871947_ Conceptualising_ cyber_ arms_ races

Crane, C. C.; Lynch, M. E.; Sheets, J. J. and Reilly, Sh. P. (2019). *A Return to Information Warfare*. The United States Army War College. U.S. Army Heritage and Education Center. Retrieved Oct. 21, 2019 from: https:// ahec. armywarcollege. edu/documents/A_Return_to_Information_Warfare.pdf

Cutts, A. (2009). Warfare and the Continuum of Cyber Risks: A Policy Perspective. In Ch. Czosseck and K. Geers (Eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare* (pp. 66-76). Amsterdam: IOS Press

Cyberspace Policy Review. (2009). Retrieved from: https://assets.documentcloud.org/documents/2700108/Document-28.pdf

DARPA. (2008). The National Cyber Range. A National Testbed for Critical Cyber Research. Retrieved from: https://obamawhitehouse.archives.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf

Deibert, R. (2011). Tracking the Emerging Arms Race in Cyberspace. Interview interviewer: Bass. *Bulletin of the Atomic Scientists, 67*(1), pp. 1–8. Retrieved from: http://journals.sagepub.com/doi/pdf/10.1177/0096340210393703

Farwell J. P. and Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival, 53*(1), pp. 23-40. http://dx.doi.org/10.1080/00396338.2011.555586

Farwell, J. P. and Rohozinski, R. (2012). The New Reality of Cyber War. *Survival, 54*(4), pp. 107-120. https://doi.org/10.1080/00396338.2012.709391

Fergusen, B., Tall, A. & Olsen, D. (2014). National Cyber Range Overview. Paper Published in IEEE Military Communications Conference. DOI: 10.1109/ MILCOM. 2014.27. Retrieved from: https:// ieeexplore. ieee. org/ document/ 6956748/ citations#citations

Finkelstein, C. O. and Govern, K. H. (2015). Introduction: Cyber and the Changing Face

of War. *Faculty Scholarship,* Paper 1566. Retrieved from: https://scholarship.law. upenn. edu/ cgi/ viewcontent.cgi?article=2567&context=faculty_scholarship

Gertz, B. (2012, Sep. 30). White House Hack Attack. Retrieved from The Washington Free Beacon: http://freebeacon.com/white-house-hack-attack/.

Gomez, M. N. A. (2016). Arming Cyberspace: The Militarization of a Virtual Domain. *Global Security and Intelligence Studies, 1*(2), pp. 42-65. Retrieved from: https:// www. ibei. org/ arming- cyberspace- the- militarization- of- a-virtual-domain_ 54871.pdf

Hinsley, F. H. and Stripp, A. (2001). *Codebreakers: The Inside Story of Bletchley Park.* Oxford: Oxford University Press

Hopkins, N. (2012, Apr. 16). Militarisation of cyberspace: how the global power struggle moved online. *The Guardian*. Retrieved from: https://www.theguardian. com/ technology/2012/apr/16/militarisation-of-cyberspace-power-struggle

Kaplan, F. (2016). *Dark Territory: The Secret History of Cyber War*. New York: Simon and Schuster Paperbacks

Klare, M. T. (1978). Militarism: The Issue Today. *Bulletin of Peace Proposals,* 9(2), pp. 121-128. https://doi.org/10.1177/096701067800900203

Krekel, B.; Adams, P and Bakos, G. (2012, Mar. 7). *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Report Prepared for the U.S.-China Economic and Security Review Commission). Northrop Grumman. Retrieved from: https://assets. documentcloud. org/documents/2700148/Document-66.pdf

Kosina, K. (2012). Wargames in the Fifth Domain. Master Thesis. Diplomatic Academy of Vienna. Retreived from: http://kyrah.net/da/wargames.pdf

Libicki, M. (2014). The Strategic Uses of Ambiguity in Cyberspace. In G. Siboni (Ed.), *Cyberspace and National Security; selected articles* (pp. 43-50). Tel Aviv: The Institute for National Security Studies. Retrieved from http://din-online. info/ pdf/in2e.pdf

Liff, A. P. (2012). Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies, 35*(3). pp. 401-428. http://dx.doi.org/10.1080/01402390.2012.663252

Monroe, J. S. (2009, Jun. 25). Cyber Command: Observers Worry about Unintended Consequences. Retrieved from: https:// fcw. com/ articles/2009/06/25/cyber-command-dod-nsa.aspx

Mount, M. (2010, Apr. 16). U.S. Won't Militarize Cyberspace, Nominee Says. *CNN Politics*. Retrieved from: http://edition.cnn.com/2010/POLITICS/04/16/ military. cyberspace/index.html

Olszewski, B. (2016). Militarization of Cyber Space and Multidimensionality of Security. *Journal of Science of the Military Academy of Land Forces, 48*(2), pp. (105-120). DOI: 10.5604/17318157.1216083

Pernik, P.; Wojtkowiak, J. and Verschoor-Kirss, A. (2016). National Cyber Security

Organization: United States. NATO Cooperative Cyber Defense Center for Excellence. Tallinn. Estonia. Retrieved from: https:// ccdcoe. org/ uploads/ 2018/10/ CS_organisation_USA_122015-2.pdf

Pomerleau, 2017 https://www.fifthdomain.com/workforce/career/2017/07/25/heres-how-dod-organizes-its-cyber-warriors/

Schofield, J. (2007). Introduction: Contending Views-Militarism, Militarization and War. In J. Schofield, Militarization and War (pp. 1-…). Retrieved Oct. 6 2019 from: https://link.springer.com/chapter/10.1007%2F978-1-137-07719-6_2

Shanker, Th. (2009, Jun. 23). New Military Command for Cyberspace. *The New York Times*. Retrieved from: https://www. nytimes. com/ 2009/06/24/ technology/ 24cyber. html

The National Military Strategy for Cyberspace Operations. (2006, Dec.). US Department of Defense. Retrieved from: https://www.hsdl.org/?view&did=35693

National Security Strategy. (2010 May). The White House. Seal of the President of the United States. Retrieved from:

The National Strategy to Secure Cyberspace. (2003 Feb.). Retrieved from: https://assets. documentcloud.org/documents/2700096/Document-16.pdf

The Quadrennial Defense Review Report. (Feb. 2010). Department of Defense. Retrieved from: https://archive.defense.gov/qdr/QDR%20as% 20of% 2029JAN 10%201600.pdf

The Quadrennial Homeland Security Review. (2010). Department of Homeland Security. Retrieved form: https://www. dhs. gov/ sites/ default/files/publications /2010-qhsr-report.pdf

The US International Strategy for Cyberspace. (2011, May). The White House. Washington: https:// assets. documentcloud. org/ documents/ 2700127/Document-46.pdf

Thomas, T. L. (2009). Nation-State Cyber Strategies: Examples from China and Russia. In F. D. Kramer, S. H. Starr and L. K. Wentz, *Cyberpower and National Security* (pp. 477-486). Washington, D. C.: Center for Technology and National Security Policy, National Defense University Press, Potomac Books Inc. Retrieved from: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210

Tofan, D. C.; Andrei, M. L. and Dincă, M. L. (2012). Cyber Security Policy. A methodology for Determining a National Cyber-Security Alert Level. *Informatica Economică, 16*(2): pp. 103-115. Retrieved from: https://search.proquest.com/ central/docview/1030278701/fulltextPDF/1BEA265975F04941PQ/31?accountid= 45153

Trauschweizer, I. (2018, Jan 11). Militarism. Oxford Bibliographies. Retrieved from: https://www.oxfordbibliographies.com/view/document/obo-9780199791279/obo-9780199791279-0099.xml?rskey=XOLZzu&result=3&q=militarization#firstMatch

The Comprehensive National Cyber Security Initiative. (2007). Executive Office of the

President of the United States. Retrieved from: https://obamawhitehouse.archives.gov/ sites/default/files/cybersecurity.pdf

The National Strategy to Secure Cyberspace. (2003). The White House. Retrieved from: https://assets.documentcloud.org/documents/2700096/Document-16.pdf

US Army Cyber Command. (2020). About Us. Retrieved from: https://www. arcyber.army.mil/Organization/About-Army-Cyber/

US-China Economic & Security Review Commission. (2012). *Report to Congress*. Retrieved from: https://books. googleusercontent. com/ books/ content? req= AKW5Qafv046-NM8DMEfjxsDPRt3DmSECms0B8v8X-iiVsyv7Ryo 5d0y5 Jhb YY Aft8vvcwr EsbQqaT7enKbIGPAPDdav9R3nbFufH9nhw TH8WXdLNNco 9Ami_80vfuruVpt_Zl7Y2mBVbGLtQbhtE1EDGAWAl0IvS3_M5lAdqRZi-R6zzx BwXBpY6Hbxv3gRmo-kQA1WXQXMAEjKm_ZFUojSQzcD2_PUBZuIA MFL kJ9as9jEnxKUXuijNpL455v4_ WP98GbY9hbo69RjpOLUG0Me ZSgo7So P7pA

US Department of Defense. (2010). *USCYBERCOM Fact Sheet*. Retrieved from: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf