JLCW

JOURNAL OF LAW & CYBER WARFARE

Legal Considerations on Cyber-Weapons and Their Definition

Author(s): Stefano Mele

Source: *Journal of Law & Cyber Warfare*, Vol. 3, No. 1 (Spring 2014), pp. 52-69

Published by: Lexeprint Inc.

Stable URL: https://www.jstor.org/stable/10.2307/26432559

Legal Considerations on Cyber-Weapons and Their Definition

By Stefano Mele[1]

Abstract:

The rapid evolution of scenarios and threats related to the increased use of cyber-space within the national security context, as well as an exponential spread of new and hypothetical "cyber-weapons," as described at times with sensationalist language by the media, warranted a specific analysis of the phenomenon. The article focuses on the legal aspects of the "cyber-weapons" and gives for the first time a specific legal definition of cyber-weapons. Further analysis is dedicated to analyzing the most important malwares which defined and shaped the cyber-

This paper is based on "*Cyber-weapons: legal and strategic aspects (version 2.0)*", which was published in June 2013 by the Italian Institute of Strategic Studies 'Niccolò Machiavelli' and is available at: http://www.strategicstudies.it/wp-content/uploads/2013/07/Machiavelli-Editions-Cyber-Weapons-Legal-and-Strategic-Aspects-V2.0.pdf.

[1] Stefano Mele is 'Of Counsel' to the Italian Carnelutti Law Firm, where his practice focuses on Technology, Privacy and Information Management Law. He holds a PhD from the University of Foggia. He is also Research Director on "*Cyber-security & Cyber-Intelligence*" of the Italian Military Centre for Strategic Studies (Ce.Mi.S.S.) of the Italian Ministry of Defense, and Director of the "*InfoWarfare and Emerging Technologies*" Observatory of the Italian Institute of Strategic Studies 'Niccolò Machiavelli'. He is a lecturer for several universities and military research institutions of the Italian MoD and NATO, and has authored academic papers and articles on cyber-security, cyber-intelligence, cyber-terrorism and cyber-warfare topics.

security sector in the last two years, assigning them a specific legal classification in accordance with the newly-proposed definition of the term.

I. INTRODUCTION

Since September 2010, when former US Deputy Secretary of Defense William J. Lynn III publicly defined cyber-space as "the fifth domain of warfare"[2] after ground, sea, air and space, the need to have practical rules regulating all aspects of cyber-warfare activities – especially from the point of view of international law – has become a priority for all international actors. The complexity of the subject makes this task particularly challenging. This is due to the existence of significant uncertainties and doubts over crucial and essential elements, for instance: the attacker's anonymity and traceability; the so-called "preparation of the battlefield" for cyber-operations; the description of when a cyber-attack can be defined as an "armed attack"; the proportionality of the answer compared to the attack; the rules of engagement for cyber-space; and so on. Nonetheless, the scientific community is in the process of elaborating its findings, and reference to these findings can be found in a number of

[2] William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, 89, 5 FOREIGN AFFAIRS 97 (2010); *The threat from the internet: Cyberwar*, ECONOMIST Jul. 1, 2010, http://www.economist.com/node/16481504?story_id=16481504.

commendable legal documents.[3]

However, what is still missing in this debate is a legal consideration defining the term "cyber-weapon" and when a generic software or malware can be defined as such a weapon.[4] It is crucial to define it for a correct evaluation of both the threat level from a cyber-attack, and the possible political and legal responsibilities, especially considering the costs that those governments[5] and companies[6] have to bear for each breach of the security of

[3] *See, e.g.*, HEATHER H. DINNISS, CYBER WARFARE AND THE LAWS OF WAR (2012); INTERNATIONAL GROUP OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed.) (2013); TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES (William A. Owens, Kenneth W. Dam, and Herbert S. Lin eds.) (2009); ENEKEN TIKK ET AL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS (2010); THOMAS C. WINGFIELD ET AL., INTERNATIONAL CYBER SECURITY LEGAL & POLICY PROCEEDINGS (Eneken Tikk & Anna-Maria Talihärm eds.) (2010).

[4] Even the Black's Law Dictionary has no definition for "cyber," cyber-attack, cyber-warfare or obviously for cyber-weapon.

[5] Ross Anderson et al., *Measuring the Cost of Cybercrime*, WEIS 2012 INFOSEC, 2012, http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf; DETICA & UK CABINET OFFICE, THE COST OF CYBER CRIME (2011), https://www.gov.uk/government/publications/the-cost-of-cyber-crime-joint-government-and-industry-report.

[6] Cost for the companies has been estimated to average of 8.9 million dollars in 2012, a growth of 6% compared to the previous year (8.4 million dollars), according to recent studies; *see* PONEMON INSTITUTE e SYMANTEC, 2011 COST OF DATA BREACH STUDY: UNITED STATES (2011), http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf, PONEMON INSTITUTE, 2012 COST OF CYBER CRIME STUDY: UNITED STATES (2012), http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf; PRICEWATERHOUSECOOPERS, INFORMATION SECURITY BREACHES SURVEY: TECHNICAL REPORT (2012),

their computer systems.

In brief, weapons are tools through which, in a specific context, a subject can cause damage to another subject or object, or defend itself from an attack. Almost every State over time has enacted specific legislation to regulate the use of weapons,[7] both for their classification and for their circulation. But what it is essential to highlight is that current international regulations actually do not clearly define the meaning of "cyber-weapon." They only define the generic concept of a "weapon."

From the point of view of military doctrine, even The Dictionary of Military and Associated Terms of the US Department of Defense (480 pages of definitions relevant to the defense sector) does not mention a generic concept of weapon, apart from mentioning non-lethal weapons ("*a weapon that is explicitly designed and primarily employed so as to incapacitate personnel or materiel, while minimizing fatalities, permanent injury to personnel, and undesired damage to property and the environment*"[8]) and directly defining every specific type of weapon (or weapon system) except for cyber-weapons.

http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf; UK CABINET OFFICE ET AL., KEEPING THE UK SAFE IN CYBER SPACE (2013) https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace (British Government pointed out that 93% of large companies and 76% of small companies reported a cyber-attack in 2012, with a total cost for every single break-in calculated between £.110.000 and £.250.000 for the former ones and between £.15.000 and £.30.000 for the latter ones).

[7] *See* COMMISSION TO THE EUROPEAN PARLIAMENT, ON THE IMPLEMENTATION OF COUNCIL DIRECTIVE 91/477/EEC OF 18 JUNE 1991 (2000), http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l14011_en.htm.

[8] *See* DEPT OF DEF., DOD DICTIONARY OF MILITARY AND ASSOCIATED TERMS 188 (2013), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

II. TOWARDS A LEGAL DEFINITION OF CYBER-WEAPON

To reach a precise definition of the concept of a cyber-weapon in the specific context of conflicts (warfare), it is necessary to separate it from the notion of malware typically used for cyber-crime purposes.[9] It is easy to imagine how this complicates things since, as it happens for traditional weapons, cyber-warfare activities can be performed through malware and/or information technology tools which are also used to commit mere cyber-crime actions and that do not rise to the level of acts of warfare.

A further distinction has to be made also to differentiate cyber-weapons from malware and/or information technology tools used to perform espionage activities. Espionage represents the best and the most effective way to obtain – both in war and peacetime – political, military and economic advantages on both enemies and allies. This is also valid in the case of cyber-espionage.

Indeed, over the last decade, the digitalization and centralization of information (including classified information) and the lack of cyber-security awareness and education has made it possible for espionage to become one of the most critical threats to national security and to the competitiveness of each country. Nevertheless, historically, espionage has never represented the trigger of any known inter-state conflict. As espionage activities – nowadays strongly supported by technology – are carried out by every

[9] *See* James P. Farwell & Rafal Rohozinski, *The new reality of Cyber War*, 54, 4 SURVIVAL: GLOBAL POLITICS AND STRATEGY 107 (2012) (to point out this difference, a part of the doctrine focuses on terms like "*weaponised computer code*" or "*malware employed as 'use of the force'*").

state, they are frequently tolerated by other states or, if they are carried out through extended "aggressive" strategies,[10] in the worst case they might provoke only a reaction through specific economic sanctions.[11]

Therefore, separating cyber-crime and cyber-espionage tools from the concept of cyber-weapons is a crucial element in this definition, especially because the use of a cyber-weapon could lead to the beginning of a conflict.

Having outlined the context for these considerations, it should be noted that, from an ontological point of view, a weapon can be also an abstract concept, thereby not necessarily a material one, as international and domestic legislation have considered it up to now. For these reasons, even a set of computer instructions – such as a program, or a part of a code and so on – can be considered a weapon when used in certain contexts with the specific purpose of sabotaging or damaging well-defined subjects and/or objects, through the use of certain means/tools. The aforementioned set of computer instructions can render to these kinds of intangible items the characteristic of a weapon, in this case, a cyber-weapon.

For those reasons, to reach a definition of cyber-weapon, it is necessary to focus on three essential elements:

[10] *See* DAVID WISE, TIGER TRAP: AMERICA'S SECRET SPY WAR WITH CHINA (2011); Posting of Stefano Mele to Formiche blog, http://www.formiche.net/2013/02/20/hard-power-spionaggio-cinese/ (Feb. 20, 2013).

[11] *See* Posting of Zachary K. Goldman to Snapshots blog, http://www.foreignaffairs.com/articles/139139/zachary-k-goldman/washingtons-secret-weapon-against-chinese-hackers (Apr. 8 2013) (a recent introduction to the theme of the possible reactions to cyber-espionage activities); Alina Selyukh & Doug Palmer, *U.S. law to restrict government purchases of Chinese IT equipment*, REUTERS (Mar. 27 2013) http://www.reuters.com/article/2013/03/27/us-usa-cybersecurity-espionage-idUSBRE92Q18O20130327 (concerning recent US Government policy in this sector).

[1]. **CONTEXT**: it must be the typical context of an act of cyber-warfare. This concept may be defined as a conflict among actors, both National and non-National, characterized by the use of information systems,[12] with the purpose of achieving, keeping or defending a condition of strategic, operative and/or tactical advantage.

[2]. **PURPOSE**: of causing, even indirectly, physical damage to objects or people; or of sabotaging and/or damaging in a direct way the information systems of a sensitive target of the attacked subject.

[3]. **MEAN/TOOL**: an attack performed through the use of information systems, including the Internet.

In light of the above, a cyber-weapon can be defined as:

"*A part of equipment, a device, or any set of computer instructions, used in a conflict among actors both National and non-National, with the purpose of causing (directly or otherwise) physical damage to objects or people, or of sabotaging and/or damaging in a direct way the information systems of a sensitive target of the attacked subject.*"

Moreover, if it is true that currently a highly sophisticated cyber-weapon is exclusively the product of National activities or rather the work of one or more highly specialized criminal organizations that act on behalf of a State, it is also true that in the near future, common criminality might have cyber-weapons at its disposal. As a result, this will involve a clear alteration of the "CONTEXT"

[12] The concept of information systems refers to the interactions among people, processes, data and technology. In this sense, the term is used to refer not only to information and communication technologies (ICT), but also to the way people use and interact with such technology.

element, which at the moment is closely defined to acts of cyber-warfare (political level), linking it to the economic interests typical of criminal activities (social level).

III. THE CLASSIFICATION OF STUXNET AND THE FOLLOWING MALWARE

On the basis of the definition just provided, Stuxnet can be classified as a cyber-weapon, as it represents a set of computer instructions (in the form of an executable program/malware), used in a conflict – in this case covert – among specific national actors[13] (CONTEXT), aimed at modifying in a direct way the functioning of an Iranian sensitive target (PURPOSE), damaging it through the exploitation of information systems (MEAN/TOOL).

Stuxnet can be also considered as a cyber-weapon created with the sole purpose of sabotaging and damaging the specific sensitive information system of the target. Furthermore, it maintains this quality today because of the objective difficulty of reconfiguring it ontologically as a 'non-weapon' with only non-damaging functions.

On the contrary, dual-use cyber-weapons can be defined as "*a part of equipment, a device, or any set of computer instructions*" characterized by a possible dual (non-damaging) use, with indirect or unmediated damaging side effects. There are several examples of programs created to manage and fortify a computer system's security which, if required, can be also used for offensive purposes. However, in a case where such software are actually used for offense, having the "PURPOSE" and the "MEAN/TOOL" elements unchanged, the "CONTEXT" element will have to

[13] DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER (Crown Publishers 2012).

outline the psychological layer of the intent in order to legally classify the attack correctly.

Moreover, it is interesting to highlight that, since the public disclosure of Stuxnet, many other malware programs have drawn the attention of the public, thanks to the analysis work of security companies specializing in this sector. Flame,[14] DuQu,[15] Mahdi,[16] Gauss,[17] Rocra,[18] and

[14] *Identification of a New Targeted Cyber-Attack (2012)*, IRAN NATIONAL CERT (MAHER) (May 28, 2012), http://www.certcc.ir/index.php?name=news&file=article&sid=1894&newlang=eng; *SKYWIPER* ANALYSIS TEAM, *SKYWIPER: A COMPLEX MALWARE FOR TARGETED ATTACKS* (2012), www.crysys.hu/skywiper/skywiper.pdf; Posting of Alexander Gostev to Securelist Incidents blog, https://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers (May 28, 2012 13:00 GMT); Posting of Symantec Security Response to Symantec Official Blog, http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east (May 28, 2012, 13:32:58 GMT).

[15] BOLDIZSÁR BENCSÁTH ET AL, *DUQU: A STUXNET-LIKE MALWARE FOUND IN THE WILD* (2011), www.crysys.hu/publications/files/bencsathPBF11duqu.pdf; Posting of Symantec Security Response to Symantec Official Blog, http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet (Oct. 18, 2011, 16:59:09 GMT).

[16] Kim Zetter, *Mahdi, the Messiah, Found Infecting Systems in Iran, Israel*, WIRED, Jul. 17, 2012, http://www.wired.com/threatlevel/2012/07/mahdi/; Posting of Aviv Raff to Seculert blog, http://www.seculert.com/blog/2012/07/mahdi-cyberwar-savior.html (Jul. 17, 2012).

[17] Kim Zetter, *Flame and Stuxnet Cousin Targets Lebanese Bank Customers, Carries Mysterious Payload*, WIRED, Aug. 9, 2012 http://www.wired.com/threatlevel/2012/08/gauss-espionage-tool/; Posting of GReAT to Securelist Incidents Blog, http://www.securelist.com/en/blog/208193767/ (Aug. 9, 2012, 13:00 GMT).

[18] Posting of GReAT to Securelist Incidents Blog,

FinFisher[19] are a few of the most popular malware programs, defined as "heirs" of Stuxnet by the generalist press.

Nevertheless, placing the previously mentioned malware programs into the framework of the three defining elements proposed ("CONTEXT," "PURPOSE" and "MEAN/TOOL"), there are today no other malware – publicly known – which can be classified as cyber-weapons. In the above cases, even presuming that the "CONTEXT" for each of them is an act of cyber-warfare (which may not be correct), and even having the "MEAN/TOOL" element, the "PURPOSE" of these malware programs is not one "[...] *of causing (directly or otherwise) physical damage to objects or people, or of sabotaging and/or damaging in a direct way the information systems of a sensitive target of the attacked subject.*" The common element characterizing them is another: obtaining information to carry out cyber-espionage operations. And, as stated above, espionage and cyber-espionage are not warfare.

The only exception to this assessment could come

http://www.securelist.com/en/blog/785/ (Jan. 14, 2013, 13:00 GMT); Posting on Securelist Analysis, http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation (Jan. 14, 2013).

[19] *See, e.g.*, Michael Kelley, *This Powerful Spy Software Is Being Abused By Governments Around The World*, BUSINESS INSIDER, May 2, 2013, http://www.businessinsider.com/countries-with-finfisher-spying-software-2013-5; Nicole Perlroth, *Researchers Find 25 Countries Using Surveillance Software*, NY TIMES, Mar. 13, 2013, http://bits.blogs.nytimes.com/2013/03/13/researchers-find-25-countries-using-surveillance-software/; Vernon Silver, *Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma*, BLOOMBERG, Jul. 25, 2012, http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html.

from the analysis of the malware known as Shamoon.[20] This malware program made the headlines in August 2012 for successfully hitting – *inter alia*[21] – something like 30,000 computers of the Saudi Arabian oil company Saudi Aramco, corrupting Aramco's files and deleting the Master Boot Record of the infected machines, which is the sector of the hard disk containing the sequence of commands/instructions needed to boot the operating system.

The main purpose of Shamoon was to render the targeted information systems useless. For this reason, despite being far from the sophistication and the highly specialized manpower which led to the creation of Stuxnet, Shamoon's "PURPOSE" in its simplicity was of "[...] *damaging in a direct way the information systems of a sensitive target of the attacked subject"* and of making that possible through the use of information systems ("MEAN/TOOL").

As for the verification of the "CONTEXT" element, the attack against Saudi Aramco was claimed by a hacktivist group called "Cutting Sword of Justice."[22] Therefore, considering the open source data available and

[20] *See, e.g.*, Posting of GReAT to Securelist Incidents Blog, http://www.securelist.com/en/blog/208193786/Shamoon_the_Wiper_Copycats_at_Work (Aug. 16, 2012, 16:05 GMT); Posting of Aviv Raff to Seculert blog, http://www.seculert.com/blog/2012/08/shamoon-two-stage-targeted-attack.html, (Aug. 16, 2012); Posting of Symantec Security Response to Symantec Official Blog, http://www.symantec.com/connect/blogs/shamoon-attacks (Aug. 16, 2012 15:37:11 GMT).

[21] BBC Technology, *Computer virus hits second energy firm*, BBC NEWS, Aug. 31, 2012, http://www.bbc.co.uk/news/technology-19434920.

[22] *See generally* Posting of A Guest to Pastebin, http://pastebin.com/HqAgaQRj (Aug. 15, 2012).

keeping in mind the typically ideological and propaganda aspect of hacktivist groups, currently it is not totally correct to include this attack in a cyber-warfare context. As previously stated, a cyber-warfare action can be defined as: a conflict among actors, both National and non-National, characterized by the use of information systems, with the purpose of achieving, keeping or defending a condition of strategic, operative and/or tactical advantage.

However, if in the future the Shamoon attack was to be defined in a different context, for instance if proof emerged that the attack was sponsored by a state,[23] it could be classified as a cyber-weapon.

Hence, as explained above, it is possible to outline further the typical elements of a cyber-weapon:

- its aim must be specific, therefore, the "*part of equipment, a device, or any set of computer instructions*" does not have to be created with the aim of reaching maximum diffusion, as generic malware is frequently designed (except for the case of concealment of the real purposes of an attack);
- the information systems which were hit must be classified as sensitive targets of the attacked subject;
- the purpose must be to actively penetrate the target's information systems (not just to cause a simple dysfunction) with malicious ends;
- the information systems of the target must be protected; and
- tangible or significantly detectable damage must be caused.

Relying on the above claims, it is important to underline that the technical sophistication of cyber-weapons, the target-specific attention required, as well as

[23] Digital Dao, http://jeffreycarr.blogspot.it/ (Aug. 27, 2012, 08:53 AM).

their high damage potential, requires a remarkable infusion of funds, time, and highly specialized manpower, as well as considerable intelligence information for their creation.

The need to rationalize these four elements leads one to believe that at this time a combination of efforts among one or more states and/or groups of cyber-criminals is necessary to create a cyber-weapon. The first is necessary for the economic backing and research financing, to collect intelligence on the target and the possible insertion/placement of the cyber-weapon in case of systems which are not directly connected to the Internet (as happened with Stuxnet) or easily accessible, while the second is useful to optimize time resources and for the employment of a specialized workforce.

As further proof, it is not a coincidence that the creation of Stuxnet seems to have been attributed to several non-governmental subjects, each of which was assigned to develop only a "piece" of the malware, without being aware of the range of the overall project.[24]

IV. ANTICIPATORY OUTLINES

Based on the discussion so far, cyber-crimes – above all those aimed at cyber-espionage,[25] theft of

[24] Alexander Klimburg, *Mobilising Cyber Power*, 53, 1 SURVIVAL: GLOBAL POLITICS AND STRATEGY 41 (2011).

[25] Ellen Nakashima, *U.S. said to be target of massive cyber-espionage campaign*, WASH. POST, FEB 10 2013, http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html; DEPT. OF COM. ET AL, ADMINISTRATION STRATEGY AT MITIGATING THE THEFT OF U.S. TRADE SECRETS (2013), http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

confidential information,[26] and theft of intellectual property – are and will be, at least in the short-term, the main threat[27] for information systems of both States and private companies, especially those which work in cooperation with governments. It is no coincidence that the so-called "heirs" of Stuxnet were designed exclusively to spread and infect their targets with the sole purpose of collecting information, or at most, of carrying out activities that can be classified as cyber-espionage (aimed at collecting intelligence information about potential targets of a future cyber-weapon).

If that is true, the two countries which are most likely to be the main protagonists of cyber-espionage and information theft – Russia and China – will keep on being the undisputed protagonists, also due to the collusion among leading politicians,[28] intelligence services,[29] and

[26] The latest operation which hit the headlines was called "Luckycat". Released by the security company TREND MICRO, this operation was addressed to 233 computers during 90 attacks which had as target several authorities and "sensitive" companies in Japan, India and Tibet. A report on the topic entitled *"Luckycat Redux. Inside an APT Campaign with Multiple Targets in India and Japan"* is available at http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf. Also, the graphical data about exfiltration's main operations of sensitive and reserved data which are currently known can be helpful. It can be found at http://blog.trendmicro.com/global-targets-infographic/ .

[27] JAMES R. CLAPPER, WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY FOR THE SENATE SELECT COMMITTEE ON INTELLIGENCE (2012) http://www.dni.gov/files/documents/Newsroom/Testimonies/20120131_testimony_ata.pdf; Posting of Emil Protalinski to ZDNet Security Blog, http://www.zdnet.com/blog/security/richard-clarke-china-has-hacked-every-major-us-company/11125, (Mar. 27, 2012, 13:04 GMT).

[28] *See* Klimberg, *supra* note 24.

groups of cyber-criminals[30] or hacker patriots.[31]

As things stand now, it could be argued that both Russia and China are and probably will increasingly be the two most active states in the field of cyber-warfare.[32] Together with the United States and Israel, they will carry out a leading role in the conception, development, creation and employment of the next generations of cyber-weapons, or rather of software able to "self-learn" in real time how to sabotage or damage a target system directly from the analysis of the target system – and consequently to attack it autonomously.[33]

[29] It will suffice to consider that in 2006 more than 78% of the 1,016 Russian political leaders were previously working for organizations affiliated to KGB and to FSB. For further research, *see* Interview by Evgenia Albats with Olga Kryshtanovskaya on Echo of Moscow, Feb. 4, 2007.

[30] Above all the *Russian Business Network* (RBN). For further research, *see generally* DAVID BIZEUL, RUSSIAN BUSINESS NETWORK STUDY http://www.bizeul.org/files/RBN_study.pdf (2007); *A walk on the dark side*, THE ECONOMIST, Aug. 30, 2007, http://www.economist.com/node/9723768?story_id=9723768.

[31] People who have high technical capacities and are politically motivated to act for and in the interest of their country.

[32] BRYAN KREKEL ET AL, OCCUPYING THE INFORMATION HIGH GROUND: CHINESE CAPABILITIES FOR COMPUTER NETWORK OPERATIONS AND CYBER ESPIONAGE (2012); U.S.-CHINA ECON. & SEC. REV. COMMISSION, 2009 REPORT TO CONGRESS (2009); U.S. DEPT. OF DEF., MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA (2013), http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf.

[33] THOMAS RID, CYBER WAR WILL NOT TAKE PLACE 54 (Hurst & Co. Publishers 2013).

Finally, a medium-term analysis shows that Iran[34] will play a role very similar to the ones currently carried out by Russia and China, and, though to a lesser extent, North Korea.[35] Both countries show an increased interest in these fields and are increasing their investments in economic and human resources to this end.

[34] Among the many articles and latest news: Kenneth Corbin, *Iran Is a More Volatile Cyber Threat to U.S. than China or Russia*, CIO.COM, Mar. 21, 2013, http://www.cio.com/article/730589/Iran_Is_a_More_Volatile_Cyber_Threat_to_U.S._than_China_or_Russia; S. Isayev & T. Jafarov, *Iran establishes supreme cyberspace council*, TREND.AZ, Mar. 7, 2012, http://en.trend.az/regions/iran/2001057.html; *Iran cyber defense headquarters makes local mail servers*, PRESS TV, Mar. 17, 2012, http://www.presstv.ir/detail/232105.html; Amy Kellogg, *Iran is Recruiting Hacker Warriors for its Cyber Army to Fight 'Enemies'*, FOXNEWS.COM Mar. 14, 2011, http://www.foxnews.com/world/2011/03/14/iran-recruiting-hacker-warriors-cyber-army/.

[35] U.S. OFFICE OF THE SECRETARY OF DEFENSE, MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA (2013), http://www.defense.gov/pubs/ReporttoCongressonMilitaryandSecurityDevelopmentsInvolvingtheDPRK.pdf; Ed Barnes, *North Korea's Cyber Army Gets Increasingly Sophisticated*, FOXNEWS.COM, May 17, 2011, http://www.foxnews.com/world/2011/05/17/north-koreas-cyber-army-gets-increasingly-sophisticated/; Dan Dieterle, *North Korea's Cyber War Forces*, INFOSEC ISLAND, Mar. 6, 2012, http://infosecisland.com/blogview/20532-North-Koreas-Cyber-War-Forces.html; *North Korea has 30,000 electronic warfare agents*, THE KOREA HERALD, May 18, 2011, http://www.koreaherald.com/national/Detail.jsp?newsMLId=20110518000723; Sangwon Yoon, *North Korea recruits hackers at school*, AL-JAZEERA, Jun. 20, 2011, http://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html.

V. CONCLUSIONS

The protection of national strategic assets, which nowadays can be compromised by a cyber-attack, almost instantly is and must always be the priority, whether we are facing cyber-warfare activities or actions aimed exclusively at seizing the sensitive and/or classified information of governments.

A correct understanding of the concept of cyber-weapon – including a legal definition – is the main and urgent objective that must be achieved. This will allow the evaluation of both the threat level coming from cyber-attacks, and the direct political and legal responsibilities of the authors of the attack.

Furthermore, only with the appropriate attention on legal definitions and the creation of a commonly accepted set of rules, will it be possible to start addressing these issues which urgently require a very pragmatic response. The urgency is apparent, especially now that, due to the lack of valid technical (traceability of attacks) and judicial (responsibility for the attacks) answers, the majority of the governments are trying to speed up the innovative and takeover processes of cyber-weapons, in order to easily steal confidential information, but also to possibly sabotage or damage the enemy's military networks.[36]

The challenges that governments, the Armed Forces and National Security Institutions are, and will be, facing increasingly in the field of cyber-security and cyber-intelligence are certainly as complex as they are fascinating. Cyber-weapons require an adaptive response

[36] Ellen Nakashima, *U.S. accelerating cyberweapon research*, WASH. POST, Mar. 18, 2012, http://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html.

approach, which includes both the technical-technological research sector and the strategic, operational and tactical sectors. For the first time, the latter sectors are experiencing their exposure and vulnerability to vanishing of their typical sectorial partition right through to the Internet and technologies.

Defining with certainty what constitutes a cyber-weapon, and when a cyber-attack on sensitive targets can be considered as a 'use of force', or an 'armed attack' represents a common priority by now, especially in the modern Western world which is interconnected and bases its entire social welfare on the functioning of information technologies. The US Government began paving the path,[37] but an increasing number of countries have started to modify their strategies even providing for offensive military operations via cyberspace.[38] The future of cyber-attacks will be a challenging one.

[37] DEPT. OF DEF., STRATEGY FOR OPERATING IN CYBERSPACE (2011), http://www.defense.gov/news/d20110714cyber.pdf; David E. Sanger & Thom Shanker, *Broad Powers Seen for Obama in Cyberstrikes*, NYTIMES, Feb. 3, 2013, http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html.

[38] CONG. REC. VOL. 157, NO. 190, P. H8356-H8726 (Dec. 12 2011), http://www.fas.org/irp/congress/2011_cr/cyberwar.html; AUSTL. GOVT. DEPT. OF DEF., DEFENCE WHITE PAPER 2013 (2013), http://www.defence.gov.au/WhitePaper2013/docs/WP_2013_web.pdf; GOUVERNEMENT FRANÇAIS, LIVRE BLANC SUR LA DÉFENSE ET LA SÉCURITÉ NATIONALE 2013 (2013), http://www.elysee.fr/assets/pdf/Livre-Blanc.pdf.