Observatory
Infowarfare and
Emerging Technologies

ISTITUTO ITALIANO
DI STUDI STRATEGICI
ITALIAN INSTITUTE
OF STRATEGIC STUDIES
Niccolò Machiavelli

Cyber-weapons:
legal and strategic aspects

Version 2.0

Stefano Mele

June 2013

Machiavelli Editions

www.strategicstudies.it

ISTITUTO ITALIANO DI STUDI STRATEGICI

ITALIAN INSTITUTE OF STRATEGIC STUDIES

Niccolò Machiavelli

AUTHOR

Stefano Mele

Coordinator of the "InfoWarfare and Emerging Technologies" Observatory of the Italian Institute of Strategic Studies 'Niccolò Machiavelli'.

Lawyer of Carnelutti Law Firm, where his activity mainly focuses on Information and Communication Technology Law, Privacy, Security and Intelligence.

Research Director on "Cyber-security & Cyber-Intelligence" of the Italian Military Centre for Strategic Studies (Ministry of Defense).

He is a Lecturer for several universities and military research institutions.

He holds a PhD from the University of Foggia.

AUTHOR'S NOTE

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 an update of the analysis which was released only a year ago.

The study focuses on a revision, and an in-depth examination of the legal definition of the term "cyber-weapon", taking into consideration the changes which have characterized this field over the past year. Further analysis is dedicated to analyzing the most important malwares which defined and shaped the cyber security sector in 2012, assigning them a specific legal classification in accordance with the newly- proposed definition of the term.

Furthermore, the author wishes to expresses his gratitude to the military personnel who, over the course of the year, have contributed with their invaluable comments to lectures, meetings, workshops and briefings, providing the groundwork for this revision.
A particular mention is extended, to the women and men serving with the Defense Staff and with the Training and Research Institutes of the Department of Defense.

A personal note of gratitude goes to Dr. Claudio Neri, Mr. Giovanni Nacci, Prof. Pierluigi Perri, Prof. Umberto Gori, Ms. Gaja Pellegrini-Bettoli and to Dr. Francesca Bosco for their precious support.

1.0 Stuxnet

1.1 Introduction

The use of the Stuxnet[1] malware to attack depleted uranium plants in Iran[2], marked a definite turning point in the debate about the possibility, until then merely theoretic, to physically damage a country's critical infrastructure by exploiting the information systems operating within its infrastructure.

The first version of the malware started to spread in June 2009[3], but it was only in mid-June 2010 that, what later became known as "Stuxnet", was detected by the Belarusian Company VirusBlokAda. Stuxnet targeted the industrial information systems developed by the German company Siemens which were used by the Iranian government in some of its uranium-enrichment plants. While the malware has not been the first case of an attack against these types of information systems[4], it is the first – publicly recognized software – which was specifically designed to spy, sabotage, reprogram and physically damage its target in a self-contained and automatic way[5].

1. For a full and complete analysis on technical aspects of Stuxnet malware, inter alia, Marco De Falco, "Stuxnet Facts Report - A Technical and Strategic Analysis", NATO CCD COE Publications, 2012.

2. Paul Woodward, "Iran confirms Stuxnet found at Bushehr nuclear power plant", 2010, at http://warincontext.org/2010/09/26/iran-confirms-stuxnet-found-at-bushehr-nuclear-power-plant/; Foreign Policy, "6 mysteries about Stuxnet", 2010, at http://blog.foreignpolicy.com/posts/2010/09/27/6_mysteries_about_stuxnet.

3. Actually, a recent report by Symantec shows that a version 0.5 of Stuxnet was already operating at least since 2007. For further research: http://www.symantec.com/connect/blogs/stuxnet-05-missing-link.

4. Computer World, "Siemens: Stuxnet worm hit industrial systems", 2010, at http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems.

5. For further research on the subject under different points of view, Symantec, "W32 Stuxnet Dossier", 2011, at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; CSFI, "Stuxnet Report", 2010, at http://www.csfi.us/?page=stuxnet; Antiy Cert, "Report on the Worm Stuxnet Attack", 2010, at http://www.antiy.net/en/research/report_on_the_worm_stuxnet_attack.html; Eric Byres, "Analysis of the Siemens WinCC / PCS7 "Stuxnet" Malware for Industrial Control System Professionals", 2010, at http://www.tofinosecurity.com/professional/siemens-pcs7-wincc-malware; ESET, "Stuxnet Under the Microscope", 2010, at http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; Ralph Langner, "How to Hijack a Controller. Why Stuxnet Isn't Just About Siemens' PLCs", 2011, at http://www.controlglobal.com/articles/2011/IndustrialControllers1101.html.

While Microsoft Windows systems have been the main vehicle of infection, after the contamination, Stuxnet spread indiscriminately to hundreds of millions of information systems. The malware, which automatically stopped spreading on June 24, 2012[6], was programmed to activate itself only when coming into contact with a SCADA[7] system equipped with Siemens WinCC[8], PCS7 or STEP7[9].

Stuxnet's primary target was to reach the PLC[10] (Programmable Logic Controller) of the SCADA information systems of the Iranian uranium enrichment plants, to infect the "Step-7" application used for their programming,[11] and to reprogram the turbines' rotation speed to damage them.

According to open source data, Stuxnet succeeded in its purpose: rapidly infecting more than 100.000 targeted systems, more than a half of which were located on Iranian territory[12].

1.2 Stuxnet: preliminary discussion points for strategic consideration

The international community of experts agrees on the following evaluation: the process which brought to Stuxnet required a considerable workforce[13] commitment – a period between six[14] and twelve[15] months – with a team of programmers specialized in different fields with specific knowledge of the systems' functioning and industrial processes managed by the target[16].

Stuxnet was certainly a complex malware, but it was less advanced than the media led the general public[17] believe. Nonetheless, many security companies and independent security experts agree on assigning the malware's authorship to one or more States with **considerable funds**[18], **strong political-military motivations**[19] and **significant**

6. Costin Raiu, "The Day The Stuxnet Died", at http://www.securelist.com/en/blog/208193609/The_Day_The_Stuxnet_Died.

7. In short, SCADA systems (Supervisory Control and Data Acquisition), are all those distributed information systems aimed at monitoring and controlling physical systems electronically.

8. Ralph Langner, "Ralph's Step-By-Step Guide to Get a Crack at Stuxnet Traffic and Behavior", 2010, at http://www.langner.com/en/2010/09/14/ralphs-step-by-step-guide-to-get-a-crack-at-stuxnet-traffic-and-behavior/.

9. Nicolas Falliere, "Stuxnet Infection of Step 7 Projects", 2010, at http://www.symantec.com/connect/blogs/stuxnet-infection-step-7-projects.

10. Computers used for a program execution to elaborate digital and analog signals deriving from sensors direct to the actuators of a factory.

11. Steven Cherry and Ralph Langner, "How Stuxnet Is Rewriting the Cyber-terrorism Playbook", 2010, at http://spectrum.ieee.org/podcast/telecom/security/how-stuxnet-is-rewriting-the-cyberterrorism-playbook

12. Symantec, "W32 Stuxnet Dossier", 2011, cit..

13. Marco De Falco, "Stuxnet Facts Report - A Technical and Strategic Analysis", cit..

14. Dale Peterson, "Offensive Cyber Weapons: Construction, Development, and Employment", The Journal of Strategic Studies, 2013, at http://www.tandfonline.com/doi/full/10.1080/01402390.2012.742014; The Guardian, "Stuxnet worm is the 'work of a national government agency'", 2010, at http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency.

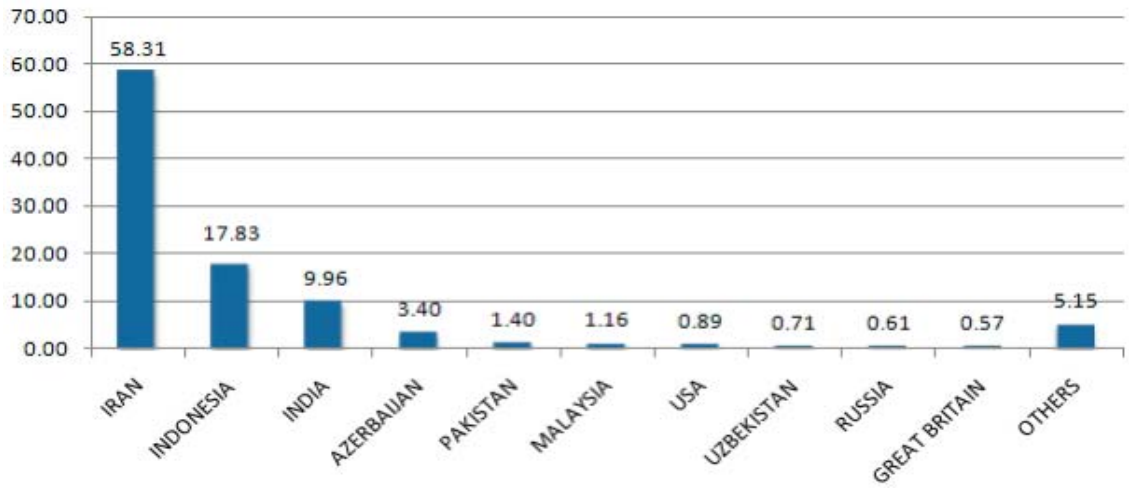
15. Wired, "Blockbuster Worm Aimed for Infrastructure, But No Proof Iran Nukes Were Target", 2010, at http://www.wired.com/threatlevel/2010/09/stuxnet/.

16. Computer World, "Is Stuxnet the 'best' malware ever?", 2010, at http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever_.

17. Lukas Milevski, "Stuxnet and Strategy: A Space Operation in Cyberspace?", in JFQ (Joint Force Quarterly), issue 63, 4th quarter, 2011.

18. NYTimes, "A Silent Attack, but Not a Subtle One", 2010, at http://www.nytimes.com/2010/09/27/technology/27virus.html.

19. BBC, "Stuxnet worm 'targeted high-value Iranian assets'", 2010, at http://www.bbc.co.uk/news/technology-11388018.



intelligence information at their disposal. At the moment, Israel[20] and the United States[21] would be the main suspects/culprits, while an involvement of Russian cyber-criminality in one or more programming phases of some parts[22] of Stuxnet itself cannot be excluded.

At first the debate appeared focused on the technical-tactical aspects of cyber-weapons, however it's the strategic and juridical aspects which are of primary importance and warrant an urgent response from specialists and decision-makers.

Firstly, it is essential to highlight that the most relevant strategic aspect of Stuxnet is the convergence between **actions typical of cyber-crime** and **State interests**. Through Stuxnet, a new trend has consolidated and taken on a "tangible" form. The trend shows the commitment of national governments to capitalize on their investments in cyber-security in technical, technological and know-how research. These activities are carried out primarily by groups of independent researchers and, increasingly, by groups of cyber-criminals[23]. Nearly all the most significant actions carried out in cyber-space from 2006 up to now[24] are closely related to research, techniques and programming codes

20. The Economist, "A cyber-missile aimed at Iran?", 2010, at http://www.economist.com/blogs/babbage/2010/09/stuxnet_worm.

21. David E. Sanger, "Confront and Conceal. Obama's Secret Wars and Surprising Use of American power", Crown Publishers, 2012, pag. 188; Ralph Langner, "Cracking Stuxnet, a 21st-century cyber weapon", 2011, at http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html.

22. The Diplomat, "Was Russia Behind Stuxnet?", 2011, at http://the-diplomat.com/2011/12/10/was-russia-behind-stuxnet/.

23. Finally it is the case, for instance, of that cyber-espionage operation named "Red October". Its main targets were the information systems and the confidential/classified data contained in some information systems deriving from Governments, embassies, research centers and companies operating in the energy, oil and gas sectors of 69 countries all over the world. The operation does not appear to have been an activity financed by a State, considering the elements so far analyzed by Kaspersky Lab, which firstly highlighted this impressive electronic spying network. More likely, this operation can be attributed to a Russian organized criminal group, aimed at stealing classified information to be sold on the market to the highest bidder. For further research, Securelist, "The Red October Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies", at http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies, 2013; Stefano Mele, "I misteri di Red October", at http://www.formiche.net/2013/01/16/kaspersky-lab-spionaggio/, 2013.

24. CSIS (Center for Strategic and International Studies), "Significant Cyber Incidents", updated on March, 16, 2012, at http://csis.org/publication/cyber-events-2006

developed by the international community of cyber-criminals[25]. Furthermore, another trend is that these cyber-criminals are becoming the main "beneficiaries" of governments[26] which subcontract them to carry out illegal operations in cyber space[27].

No wonder that, as time passes, a real "black market" of computer vulnerabilities[28] found in the most commonly used software has developed, mainly targeting vulnerabilities which are not yet publicly known (the so-called "zero-day" or "0-day"). The following table offers an indication of the economic volumes related to this illegal market. The table below was published as a result of a recent Forbes[29] research, related to an indicative price range for every single zero-day detected and put up for sale on the market.

ADOBE READER	$5,000-$30,000
MAC OSX	$20,000-$50,000
ANDROID	$30,000-$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000-$100,000
MICROSOFT WORD	$50,000-$100,000
WINDOWS	$60,000-$120,000
FIREFOX OR SAFARI	$60,000-$150,000
CHROME OR INTERNET EXPLORER	$80,000-$200,000
IOS	$100,000-$250,000

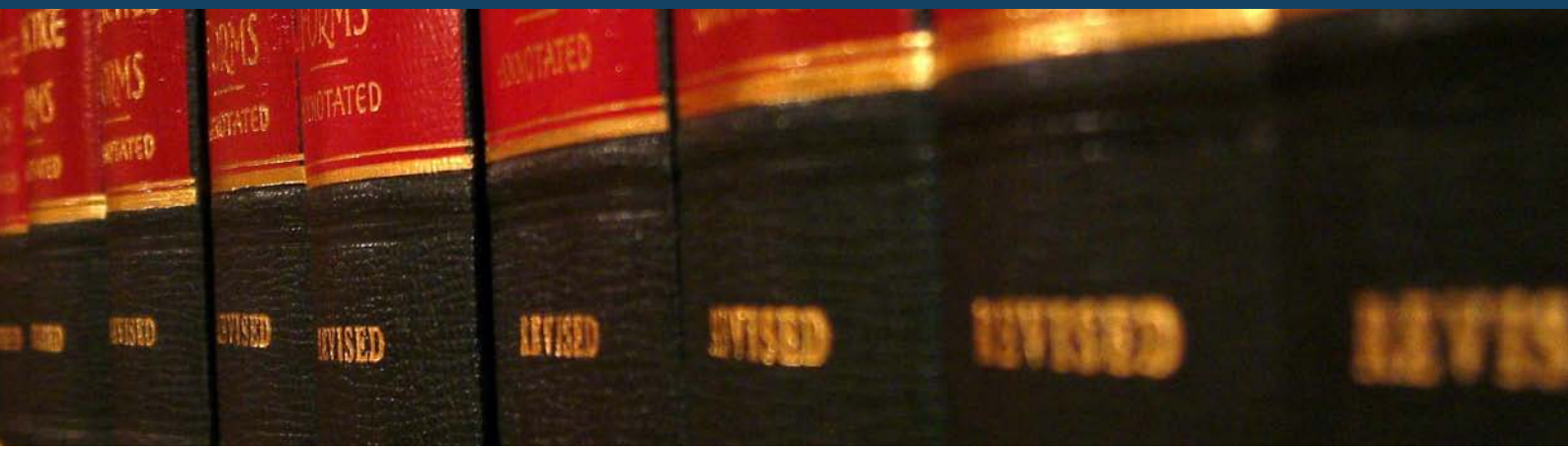
25. James P. Farwell & Rafal Rohozinski, "Stuxnet and the Future of Cyber War", in Survival: Global Politics and Strategy, vol. 53, no. 1, February–March 2011.

26. Mandiant, "APT1: Exposing One of China's Cyber Espionage Units", 2013, at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf; Northrop Grumman Corp, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage", 2012, at http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf; Mark A. Stokes and L.C. Russell Hsiao, "Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests", 2012, at http://project2049.net/documents/countering_chinese_cyber_operations_stokes_hsiao.pdf; Office of the National Counterintelligence Executive (ONCIX), "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011", 2011, at http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf; US–China Economic and Security Review Commission, "2009 Report to Congress", 2009, at http://www.uscc.gov/annual_report/2009/annual_report_full_09.pdf; Alexander Klimburg, "Mobilizing Cyber Power", in Survival: Global Politics and Strategy, vol. 53, no. 1, February–March 2011.

27. Verizon, "2013 Data Breach Investigations Report", 2013, at http://www.verizonenterprise.com/DBIR/2013/; Stefano Mele, "Cyberwarfare and its damaging effects on citizens", 2010, at http://www.stefanomele.it/public/documenti/185DOC-937.pdf.

28. Reuters, "Special Report: U.S. cyberwar strategy stokes fear of blowback", 2013, at http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510.

29. Forbes, "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits", 2012, at http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/. For further research, one of the first works aimed at introducing and quantifying black market exploits is by Charles Miller, "The legitimate vulnerability market: the secretive world of 0-day exploit sales", 2007, at http://securityevaluators.com/files/papers/0daymarket.pdf. See also Ryan Gallagher, "Cyberwar's Gray Market. Should the secretive hacker zero-day exploit market be regulated?", 2013, at http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html.



2.0 Legal considerations about cyber-weapons and their definition

2.1 Introduction

Since September 2010, when the former US Secretary of Defense, William J. Lynn III, publicly defined cyber-space as "*the fifth domain of warfare*"[30] after ground, sea, air and space, the need to have practical rules regulating all aspects related to these actions – especially from the point of view of international law – has become a priority. 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", 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 and so on.

Nonetheless, the scientific community is in the process of elaborating its findings, albeit not in a streamlined way. Reference to these findings can be found in a number of commendable legal documents[31].

What is still missing, however, is a legal consideration defining the term "cyber-weapon" and when a generic software or malware can be defined as a weapon. It is crucial to define the concept of cyber-weapon from a legal point of view for a correct evaluation of both the threat level from a cyber-

30. William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy", in Foreign Affairs, 2010, pp. 97–108; Economist, "The threat from the internet: Cyberwar", 2010, at http://www.economist.com/node/16481504?story_id=16481504.

31. Among the numerous articles published, for further research, works which deal with a part of those legal themes related to the subject. See Michael N. Schmitt, "Tallinn Manual on the International Law Applicable to Cyber Warfare", Cambridge University Press, 2013; Heather Harrison Dinniss, "Cyber Warfare and the Laws of War", Cambridge University Press, 2012; EnekenTikk, Anna-Maria Talihärm, "International Cyber Security Legal & Policy Proceedings", CCD COE Publications, 2010; EnekenTikk, KadriKaska, LiisVihul, "International Cyber Incidents: Legal Considerations", CCD COE Publications, 2010; William A. Owens, Kenneth W. Dam, Herbert S. Lin, "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities", National Academies Press, 2009.

attack and the possible political and legal responsibilities. Defining a cyber-weapon is of the utmost importance also considering the costs that governments[32] and companies[33] have to bear for each breach of the security of 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 they can also used as protection against an attack.

Almost every State over time has equipped itself with specific legislation regulating the use of weapons[34], both for their classification and circulation.

From a non-military point of view, for instance, the Italian Criminal Code, articles 585 and 704, considers as weapons:

[1]. fire arms and any weapon designed to harm another a person;

[2]. any tools suitable to damage/harm, whose detention is undeniably forbidden by law and with no justifiable reason;

[3]. bombs, any kind of machine or shell containing explosive material, asphyxiating or blinding gases, assimilated to weapons.

Tools which may be used to bring about harm/damage, but which were created for other purposes, for example knives, clubs, chains, hammers, etc. can be considered "improper" weapons.

It is essential to highlight that current international regulations do not clearly define the meaning of a cyber-weapon. They only define the generic concept of weapon.

From the point of view of military doctrine, even The Dictionary of Military and Associated Terms[35] of the US Department of Defense, 550 pages of relevant definitions in the defense sector, does not mention a generic concept of weapon, apart from mentioning non-lethal[36] weapons and directly defining every specific type of weapon (or weapon system) except for cyber-weapons.

32. Ross Anderson, Chris Barton, Rainer Bohme, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, Stefan Savage, "Measuring the Cost of Cybercrime", 2012, at http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf; UK Cabinet Office, "The cost of cyber crime", 2011, at https://www.gov.uk/government/publications/the-cost-of-cyber-crime-joint-government-and-industry-report.

33. Cost for the companies which has been estimated to be an average of 8.9 million dollars in 2012, with a growth of 6% compared to the previous year (8.4 million dollars), according to a recent American study. For further research, Ponemon Institute, "2012 Cost of Cyber Crime Study: United States", 2012, at http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf. To consult the 2011 study, Ponemon Institute e Symantec, "2011 Cost of Data Breach Study: United States", 2012, at http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf.
British Government instead, 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 breaking calculated between £.110.000 and £.250.000 for the first ones and between £.15.000 and £.30.000 for the latter ones. For further research, https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace and PricewaterhouseCoopers, "Information security breaches survey 2012. Technical report", 2012, at http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf.

34. The reference legislation for the European Community is the Council Directive 91/477/CEE of 18 Jun 1991 and its following amendments, related to the control of acquisition and possession of weapons, which can be found at http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l14011_en.htm.

35. DoD Dictionary of Military and Associated Terms, at http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

36. Defined as "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".

2.2 Towards a legal definition of cyber-weapon

To reach a precise definition of the concept of **cyber-weapon in the specific context of conflicts (warfare)**, it is necessary to separate it from the legal concept of malware, typically used for criminal purposes[37]. It is easy to imagine how this complicates things since, as it happens for traditional weapons, a cyber-warfare case performed through malware and/or information tools, which are also used to commit mere criminal actions, might amount to a criminal offence.

On the other hand, a further distinction has to be made to differentiate cyber-weapons from malware and/or information tools used to perform espionage activities exploiting cyber-space and technology. Espionage, represents the best and the most effective tool to obtain – both in war and peace time – political, military and economic advantages on both enemies and allies. This is also valid in the case of cyber-espionage. Nevertheless, historically, espionage itself never represented the trigger of any inter-state conflict. Yet, over the last decade the digitalization of information (including confidential information), its subsequent centralization and the poor perception of the risks deriving from the use of information technologies, has made it possible for espionage to become one of the most critical threats to national security and to the competitiveness of a country's system. As espionage activities – nowadays strongly supported by technologies – are carried out by every State, they are frequently tolerated or, in case they are carried out through extended "aggressive" strategies[38], in the worst case they can provoke a reaction through specific economic sanctions[39].

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** can be considered a weapon, such as a program, or a part of a code and so on, when used in certain contexts with the purpose of sabotaging or damaging specific subjects and/or objects, through the use of certain means/tools. The above-mentioned set of computer instructions can render these kinds of intangible items the characteristic of a weapon, in this case a cyber-weapon.

37. 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'". Inter alia , see James P. Farwell & RafalRohozinski, "The new reality of Cyber War", in Survival: Global Politics and Strategy, vol. 54, no. 4, August–September 2012.

38. Stefano Mele,"La strategia hard power dello spionaggio cinese", 2013, at http://www.formiche.net/2013/02/20/hard-power-spionaggio-cinese/; David Wise, "Tiger Trap. America's Secret Spy War with China", Houghton Mifflin Harcourt, 2011.

39. For a recent introduction to the theme of the possible reactions to cyber-espionage activities, inter alia, see Zachary K. Goldman, "Washington's Secret Weapon Against Chinese Hackers", 2013, at http://www.foreignaffairs.com/articles/139139/zachary-k-goldman/washingtons-secret-weapon-against-chinese-hackers. Concerning recent policy of the US Government in this sector, see Reuters, "U.S. law to restrict government purchases of Chinese IT equipment", 2013, at http://www.reuters.com/article/2013/03/27/us-usa-cybersecurity-espionage-idUSBRE92Q18O20130327.

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

[1]. the **CONTEXT**, it must be the typical context of a cyber-warfare act. This concept may be defined as a conflict among actors, both National and non-National, characterized by the use of technological information systems[40], with the purpose of achieving, keeping or defending a condition of strategic, operative and/or tactical advantage.

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

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

These seem to be the only elements used to qualify or not even a set of computer instructions as a weapon.

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, EVEN INDIRECTLY, A PHYSICAL DAMAGE TO EQUIPMENT OR PEOPLE, OR RATHER OF SABOTAGING OR DAMAGING IN A DIRECT WAY THE INFORMATION SYSTEMS OF A SENSITIVE TARGET OF THE ATTACKED SUBJECT."

Moreover, as examined later in this study, if it is true that currently a highly sophisticated cyber-weapon – as Stuxnet – is exclusively the product of National activities or rather the work of one or more highly specialized criminal organizations which act on behalf of a State, 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" element**, at the moment closely defined, to acts of cyber-warfare (**political level**), linking them to the economic interests (**social level**) typical of criminal activities.

2.3 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[41] (**CONTEXT**), aimed at modifying in a direct way the functioning of an Iranian critical target (**PURPOSE**), damaging it through the exploitation of technological information systems (**MEAN/TOOL**).

Stuxnet can be considered as a so-called **"proper" cyber-weapon**, because it was created, with the sole purpose of sabotaging and damaging the specific sensitive information system of the target. Furthermore, it maintains this quality as we consider the objective difficulty of reconfiguring it ontologically as a "non-weapon", redirecting it solely to non-damaging functions.

40. The concept of information system refers to the interaction 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.

41. David E. Sanger, "Confront and Conceal. Obama's Secret Wars and Surprising Use of American power", cit..

On the contrary, **"improper" cyber-weapons** can be found in "*a part of equipment, a device or any set of computer instructions*" characterized by a possible dual-use, with indirect or planned effects. There are several examples of programs created to manage and harden the computer systems' security which, if required, can be used for offensive purposes. However, in case such software are actually used, having the "PURPOSE" and the "MEAN/TOOL" elements unchanged, the "context" element will have to 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 malware suddenly draw the attention of the public opinion thanks to the analysis work of some security companies specialized in this sector. **Flame**[42], **DuQu**[43], **Mahdi**[44], **Gauss**[45], **Rocra**[46], **FinFisher**[47], are the names of some of the most popular malware, defined as "heirs/children" of Stuxnet by the generalist press.

Nevertheless, placing the technical outcomes of these malware in the framework of the three defining elements proposed ("CONTEXT", "PURPOSE" and "MEAN/TOOL"), it is easy to exclude that currently there are other malware – publicly known – which can be classified as cyber-weapons. In the above-mentioned cases, even presuming that the "CONTEXT" for each of them is a cyber-warfare act (which, however, is not correct), having the "MEAN/TOOL" element, the "PURPOSE" of these malware, however, is not "[...] o*f causing, even indirectly, a physical damage to equipment or people, or rather of sabotaging or damaging in a direct way the information systems of a sensitive target of the attacked subject*". The common element characterizing them is another one: obtaining information to carry out cyber-espionage operations.

42. Iran National CERT (MAHER), "Identification of a New Targeted Cyber-Attack", 2012, at http://www.certcc.ir/index.php?name=news&file=article&sid=1894&newlang=eng; Alexander Gostev, "The Flame: Questions and Answers", 2012, at https://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers; Laboratory of Cryptography of Systems Security (CrySyS), "sKyWIper: A Complex Malware for Targeted Attacks", 2012, at www.crysys.hu/skywiper/skywiper.pdf; Symantec, "Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East", 2012, at http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east.

43. Laboratory of Cryptography of Systems Security (CrySyS), "Duqu: A Stuxnet-like malware found in the wild, technical report", 2011, at www.crysys.hu/publications/files/bencsathPBF11duqu.pdf; Symantec, "W32.Duqu: The Precursor to the Next Stuxnet", 2011, at http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet.

44. Seculert, "Mahdi – The Cyberwar Savior?", 2012, at http://www.seculert.com/blog/2012/07/mahdi-cyberwar-savior.html; Wired, "Mahdi, the Messiah, Found Infecting Systems in Iran, Israel", 2012, at http://www.wired.com/threatlevel/2012/07/mahdi/.

45. Global Research & Analysis Team (GReAT) – Kaspersky Lab, "Gauss: Nation-state cyber-surveillance meets banking Trojan", 2012, at http://www.securelist.com/en/blog/208193767/; Wired, "Flame and Stuxnet Cousin Targets Lebanese Bank Customers, Carries Mysterious Payload", 2012, at http://www.wired.com/threatlevel/2012/08/gauss-espionage-tool/.

46. Kaspersky Lab, ""Red October" Diplomatic Cyber Attacks Investigation", 2013, at http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation; Global Research & Analysis Team (GReAT) – Kaspersky Lab, "The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies", 2013, at http://www.securelist.com/en/blog/785/.

47. Bloomberg, "Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma", 2012, at http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html; The New York Times, "Researchers Find 25 Countries Using Surveillance Software", 2013, at http://bits.blogs.nytimes.com/2013/03/13/researchers-find-25-countries-using-surveillance-software/; Business Insider, "This Powerful Spy Software Is Being Abused By Governments Around The World", 2013, at http://www.businessinsider.com/countries-with-finfisher-spying-software-2013-5.

The only exception to this assessment could come from the analysis of the malware known as **Shamoon**[48]. This malware made the headlines in August 2012 for successfully hitting – *inter alia*[49] – something like 30.000 (thirty thousands) computers of the Saudi Arabian oil company Saudi Aramco, corrupting its 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 start 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 from the workforce employment which led to the creation of Stuxnet, in its "simplicity" Shamoon's "PURPOSE" 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 technological information systems ("MEAN/TOOL").

As for the verification of the "CONTEXT" element, instead, the attack against Saudi Aramco was claimed by a *hacktivist* group called "*Cutting Sword of Justice*"[50]. Therefore, considering the open source data available and keeping in mind the typically ideological and propaganda aspect of *hacktivist* groups, currently it is not correct to include this attack in a cyber-warfare context. As previously stated, the cyber-warfare context is defined as "*a conflict among actors, both National and non-National, characterized by the use of technological information systems, with the purpose of achieving, keeping or defending a condition of strategic, operative and/or tactical advantage*".

However, if in the future this attack were to be defined in a different context, for instance proof that the attack was sponsored by a State[51], at that point the Shamoon malware could be classified as a cyber-weapon.

48. Symantec, "The Shamoon Attacks", 2012, at http://www.symantec.com/connect/blogs/shamoon-attacks; Global Research & Analysis Team (GReAT) – Kaspersky Lab, "Shamoon the Wiper - Copycats at Work", 2012, at http://www.securelist.com/en/blog/208193786/Shamoon_the_Wiper_Copycats_at_Work; Seculert, "Shamoon, a two-stage targeted attack", 2012, at http://www.seculert.com/blog/2012/08/shamoon-two-stage-targeted-attack.html.

49. BBC, "Computer virus hits second energy firm", 2012, at http://www.bbc.co.uk/news/technology-19434920.

50. For further research: http://pastebin.com/HqAgaQRj.

51.Jeffrey Carr, "Who's Responsible for the Saudi Aramco Network Attack?", 2012, at http://jeffreycarr.blogspot.it/2012/08/whos-responsible-for-saudi-aramco.html.

3.0 Strategic considerations concerning cyber-weapons

3.1 The level of damage caused by cyber-weapons

After explaining what a cyber-weapon is from a legal point of view, the analysis of the malware Stuxnet provides some relevant **strategic concepts**.

The first one is certainly the **level of damage caused** by cyber-weapons. To talk about a real cyber-war[52], it is necessary that the actions carried out via cyber-space or with the use of technologies cause some real "off line"[53] damage to citizens or to sensitive objectives.

In the same way, in order to classify a cyber-weapon, it is necessary that it cause, even indirectly, physical damage to equipment or people, or rather that it sabotages or damages in a direct way the information systems of a sensitive target. For these reasons, the software used for an attack which temporarily blocks information systems, or one able to provoke a Distributed Denial of Service (DDoS), or the defacement of a site, cannot be considered as a cyber-weapon because it is unable to cause significantly detectable damage to the target.

Indeed, these types of attacks will surely

52. If properly classified and defined, a cyber-war has never taken place yet – at least at the current state. Instead, we should more correctly talk of mere acts of cyber-warfare. The US Department of Defense defines them as "the use of computers and the Internet in conducting warfare in the cyberspace". Hence, a non-definition. Probably more appropriately, as previously stated in this work, a cyber-warfare act can be defined as "a conflict among actors, both National and non-National, characterized by the use of technological information systems, with the purpose of achieving, keeping or defending a condition of strategic, operative and/or tactical advantage".

53. Stefano Mele, "Cyberwarfare and its damaging effects on citizens", cit..

cause some damage (often minimal) due to the malfunctioning of the systems, some damage to the public reputation of the attacked subject, maybe even considerable economic losses due to the interruption in the distribution of services, but all these damages, as well as many others, are nothing but an indirect consequence of a cyber-attack and not the result of a direct action of a cyber-weapon.

An exception can be found in the case of a Distributed Denial of Service (DDoS) attack carried out, for instance, against the control systems of a flying airplane, or of a running train, against the electrical system of a hospital, or rather more in general against all those information systems which, once successfully hit, have as a direct consequence a mere target system deadlock, but as indirect consequence they bring about the death of civilians[54].

In these cases, even if the software used to perform these types of attacks cannot be classified as a cyber-weapon overall, the effects caused by its use and the level of damage achieved through its use will make this hypothesis of classification possible a posteriori.

The malware Stuxnet has been created to penetrate the security of a specific target system and to reside in that very system through a rootkit[55], becoming completely invisible to detection programs. It has been also programmed to hold all the needed computer instructions to lead the target information systems to self-damage – in a direct and physically detectable way – through the corruption of the processes active on such computers. In addition, no operator noticed, not even in real time, the change undergoing the active functioning processes, due to the introduction (inside the Stuxnet code) of the possibility to violate the sensors' monitoring systems, the valves and the temperatures of the nuclear plant put under attack.

Hence, it is possible to outline the following **typical elements** of a cyber-weapon:

[1]. the aim must be specific, therefore, the "*part of equipment, a device, or any set of computer instructions*" do not have to be created with the aim of reaching their maximum diffusion, as it happens for generic malware (except for the case of concealment of the real purposes of an attack);
[2]. the information systems which have been hit must be classified as a sensitive target of the attacked subject;
[3]. the purpose must be to actively penetrate the target's information systems (not just to cause a simple dysfunction) and with malicious ends;
[4]. the information systems of the target must be protected;
[5]. tangible or significantly detectable damage must be caused.

Moreover, Stuxnet's sophistication level highlights two further issues which need to be examined. The first one is related to the **autonomy of action** power of this type of malware. In the case of Iran, since its targets were information systems disconnected from the Internet, Stuxnet was programmed to bring the whole "arsenal" required to accomplish its mission.

54. Stefano Mele, "Cyberwarfare and its damaging effects on citizens", cit..

55. A rootkit is a kind of malevolent program (malware), created to hide the existence of some processes or programs to the normal detection methods, enabling and assuring a continuous access to the target computer with the highest possible level of administration.

The second one is the almost total absence of **collateral damage**[56]. As previously maintained, the malware was accurately programmed to "start working" only when ready to infect a SCADA WinCC, PCS7 or STEP7 Siemens system, designated to manage and control well-defined industrial processes. Thereby, no damage had been detected to the information systems infected by Stuxnet after the attack and did not correspond to the target features predetermined during the programming phase.

Relying on the above-mentioned claims, it is important to underline that the technical sophistication of cyber-weapons, the target-specific attention required, as well as the high damage potential which they bring, require a remarkable amount of **funds, time**, highly specialized **manpower**, as well as considerable **intelligence information** for their creation.

The need to rationalize these four elements

leads us to believe that a "combination of efforts" among one or more States and groups of cyber-criminals is necessary to create a cyber-weapon. The first is necessary for the economic part 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 hardly 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 assigned 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[57].

56. Thomas Rid e Peter McBurney, "Cyber-weapons", in RUSI Journal, vol. 157, no. 1, 2012.

57. Alexander Klimburg, "Mobilising Cyber Power", cit..

3.2 The productivity level of the investment for cyber-weapons

Unlike conventional weapons, which have an excellent return, both in terms of efficiency and, above all, in terms of resistance of the investment productivity to the passing of time, cyber-weapons work differently and have a shorter **employment time period**. Relying on one or more vulnerabilities of the target system, which are often well-related to one another and are all necessary to achieve the final purpose, cyber-weapons can exploit a very short employment time period, proportionally decreasing with the passing of time (vulnerable programs can be updated, removed or replaced by others), multiplied for the number of vulnerabilities to be exploited for the attack to be successful.

Therefore, the **productivity factor of the investment** ("**P**") for cyber-weapons can be obtained through the following formula:

$$P_{\text{(productivity)}} = E_{\text{(employment)}} - (T_{\text{(time)}} * V_{\text{(vulnerability)}})$$

Moreover, it is necessary to highlight that the configuration of the systems to be violated can prove to be so specific that a cyber-weapon, programmed to maximize damage to a specific target, will succeed with extreme **difficulty in hitting further targets** with the same level of intensity and effectiveness, becoming inadequate for further operations. For instance, this is the case of a successfully accomplished operation, which is publicly released together with the methods and vulnerabilities used to succeed at the operation itself. In such a case, software producers will soon release a so-called "patch" to fix the vulnerabilities exploited, closing that "access way" once and for all. As a consequence, it is likely that a cyber-weapon will be used just once against a specific target or rather that it is useful for a single attack wave, provided that the attacks are carried out in a very short period of time. This is true especially in case the attack succeeds and produces damaging effects, alerting the security experts of the information systems hit, who will immediately take countermeasures, often long before the patches used to fix the vulnerabilities are released by software producers.

Summarizing these observations, it is possible to understand how the creation and the employment of cyber-weapons require superior intelligence information, time, workforce and testing resources for their creation, although being characterized by a **lower threshold of investments** (if compared to the creation of a "traditional" weapon arsenal), and ensuring the possibility **to hit targets often unreachable by other types of attacks**.

Furthermore, it is necessary to highlight that cyber-weapons:

- have a very limited employment time period, inversely proportional to the passing of time required for the employment of the cyber-weapon, to its assembly complexity and, to the security of the systems to be violated;
- are not likely to be employed again for further operations, once the target is hit, even if the new operation is addressed to different targets, because of the high visibility these kinds of attacks have nowadays on the media;

- have the power to sabotage or damage for a well-established time period[58] the sensitive information system of the target, without completely destroying it as could happen, for instance, as a consequence of a missile attack.

The high costs, the risk variables for their creation and efficiency, as well as the "limited" and anyway temporary results, lead to believe that currently **research and development activities in the field of cyber-weapons are strategically unprofitable**, unless an escalation takes place (predictable and already forecast by some experts[59]) in the power these software have to increase the damaging level and/or to make their effects last as long as possible.

In conclusion, a State-made cyber-weapon is certainly an activity to be taken into consideration and to be monitored for its future development, but it has to be defined in a correct and conscious way, far from the "sensationalist" headlines and propaganda slogans. The opportunity to successfully exploit cyber-attacks as a means to **facilitate physical attacks**[60] has to be considered of utter importance right now.

3.3 Cyber-crime, cyber-espionage and confidential information theft

Cyber-crimes need to be dealt with in a diametrically opposed way, even when they are performed, as it happens[61] more and more often, against national targets.

The economic resources, intelligence information, workforce and the phase of software testing to be employed, are often widely reduced and available to almost all the main information criminal groups, as well as to the States. The necessary information and the appropriate exploits[62] are often easily traceable directly on the Internet, or rather are available on the black market or openly available for free, on a very short term, as "modules" of known "dual use" programs for the security of information systems (i.e. Metasploit[63] and Nessus software).

However, it is necessary to point out that the **passing of time** penalizes exploit utilization, against a target system, even if with a reduction coefficient definitely lower than the one of a cyber-weapon. It is also necessary to highlight that an exploit, unlike a cyber-weapon, can often be easily reutilized for further operations, especially if addressed to different target systems.

58. IvankaBarzashka, "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme", in The RUSI Journal, 2013, Vol. 158 n. 2, pp. 48-56.

59. Stefano Mele, "Cyberwarfare and its damaging effects on citizens", cit..

60. As it seems to have happened in 2007 during the bombing of Damascus by Israeli warplanes, occurred after having disabled the Syrian warplane control systems. Richard Clarke and Robert Knake, "Cyber War. The next threat to national security and what to do about it", Harper Collins, 2010.

61. Paolo Passeri, "Cyber Attacks Timeline Master Index", 2013, at http://hackmageddon.com/cyber-attacks-timeline-master-indexes/.

62. Simplifying, an exploit is a term used to identify a group of cyber-information which, exploiting a bug or a vulnerability, leads to the acquisition of privileges or to the denial of service of a computer.

63. Let's take as an example, among all, the "Project Basecamp", which is aimed at supplying publicly and totally for free some useful ready-made modules aimed at damaging PLC systems of critical infrastructures. Details at http://www.digitalbond.com/tools/basecamp/metasploit-modules/.

3.4 Anticipatory outlines

On the basis of what stated so far, cyber-crimes – above all those aimed at **cyber-espionage**[64] as well as to the **theft of confidential information**[65] and of **intellectual property** – are and will be, at least in the short-term, the main threat[66] for information systems of both States and private companies, especially those which work in cooperation with governments.

As previously outlined, it is no coincidence that the so-called "heirs/sons" of Stuxnet were limited exclusively to spread and infect their targets with the sole purpose of collecting information, or rather, at most, of carrying out activities which can be classified as cyber-espionage aimed at collecting intelligence information about potential (next) targets of a cyber-weapon.

64. Ellen Nakashima, "U.S. said to be target of massive cyber-espionage campaign", 2013, at 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; White House, "Administration Strategy at Mitigating the Theft of U.S. Trade Secrets", 2013, at http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

65. 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. The whole report, entitled "Luckycat Redux. Inside an APT Campaign with Multiple Targets in India and Japan" is available at http://www.tradmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf. Also the graphic info about exfiltration's main operations of sensitive and reserved data which are currently known can be indicative. It can be found at http://blog.trendmicro.com/global-targets-infographic/ .

66. Richard Clarke, "China has hacked every major US company", 2012, at http://www.zdnet.com/blog/security/richard-clarke-china-has-hacked-every-major-us-company/11125; James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence", 2012, at http://www.dni.gov/files/documents/Newsroom/Testimonies/20120131_testimony_ata.pdf.

If that is true, the two countries which are more 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[67], intelligence services[68] and groups of cyber-criminals[69]/hacker patriots[70].

As things stand now, it could be argued that both Russia and China are[71] and probably will increasingly be the two most active States in the field of cyber-warfare. Together with the United Stated 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[72].

A medium-term analysis shows that **Iran**[73] will play a role very similar to the one currently carried out by Russia and China, and, though to a lesser extent, **North Korea**[74]. Both, countries show an increased interest in these fields and are incrementing their investments in economic and human resources to this end.

67. Alexander Klimburg, "Mobilising Cyber Power", cit..

68. 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, Evgenia Albats, "Siloviks in power: fears or reality?", interview with Olga Kryshtanovskaya, in Echo of Moscow, 2006.

69. Among all the Russian Business Network (RBN). For further reseach, David Bizeul, "Russian Business Network study", 2007, at http://www.bizeul.org/files/RBN_study.pdf; The Economists, "A walk on the dark side", 2007, at http://www.economist.com/node/9723768?story_id=9723768.

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

71. U.S. Department of Defense, "Military and Security Developments Involving the People's Republic of China", 2013, at http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf; Northrop Grumman Corp, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage", cit.; US–China Economic and Security Review Commission, "2009 Report to Congress", cit..

72. Thomas Rid, "Cyber war will not take place", Hurst & Co. Publishers, 2013, p. 54.

73. Among the many articles and latest news, Kenneth Corbin, "Iran Is a More Volatile Cyber Threat to U.S. than China or Russia", 2013, at http://www.cio.com/article/730589/Iran_Is_a_More_Volatile_Cyber_Threat_to_U.S._than_China_or_Russia; Trend, "Iran establishes supreme cyberspace council", 2012, at http://en.trend.az/regions/iran/2001057.html; Fars News Agency, "Iran Warns: West Using Internet for Spying", 2012, at http://english.farsnews.com/newstext.php?nn=9012151817; Press TV, "Iran cyber defense headquarters makes local mail servers", 2012, at http://www.presstv.ir/detail/232105.html; Fox News, "Iran is Recruiting Hacker Warriors for its Cyber Army to Fight 'Enemies'", 2011, at http://www.foxnews.com/world/2011/03/14/iran-recruiting-hacker-warriors-cyber-army/; The Green Voice of Freedom, "Who are the 'Iranian Cyber Army'?", 2010, at http://en.irangreenvoice.com/article/2010/feb/19/1236.

74. U.S. Office of the Undersecretary of Defense for Policy and the Defense Intelligence Agency, "Military and Security Developments Involving the Democratic People's Republic of Korea", 2013, at http://www.defense.gov/pubs/ReporttoCongressonMilitaryandSecurityDevelopmentsInvolvingtheDPRK.pdf;Infosec Island, "North Korea's Cyber War Forces", 2012, at http://infosecisland.com/blogview/20532-North-Koreas-Cyber-War-Forces.html; The Korea Herald, "North Korea has 30,000 electronic warfare agents", 2011, at http://www.koreaherald.com/national/Detail.jsp?newsMLId=20110518000723; Al-Jazeera, "North Korea recruits hackers at school", 2011, at http://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html; Fox News, "North Korea's Cyber Army Gets Increasingly Sophisticated", 2011, at http://www.foxnews.com/world/2011/05/17/north-koreas-cyber-army-gets-increasingly-sophisticated/.

4.0 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 acts, 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 an urgent and inescapable decision that must be made. This will allow to evaluate both the threat level coming from cyber-attacks, and the direct political and legal responsibilities of the authors of the attack. This is possible only in case the author of the attack is identified and legally charged for his actions, which is currently one of the most difficult problems to solve.

Nevertheless, only with the necessary clarifications of these definitions and the creation of a commonly accepted set of rules and information, will it be possible to start addressing the issues which urgently require a 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[75].

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 adjustment and feedback approaches. They include both technical and technological research sectors and the strategic, tactical and operative ones, which, for the first time, are experiencing the vanishing of their typical sectorial partition, right through to the Internet and its technology.

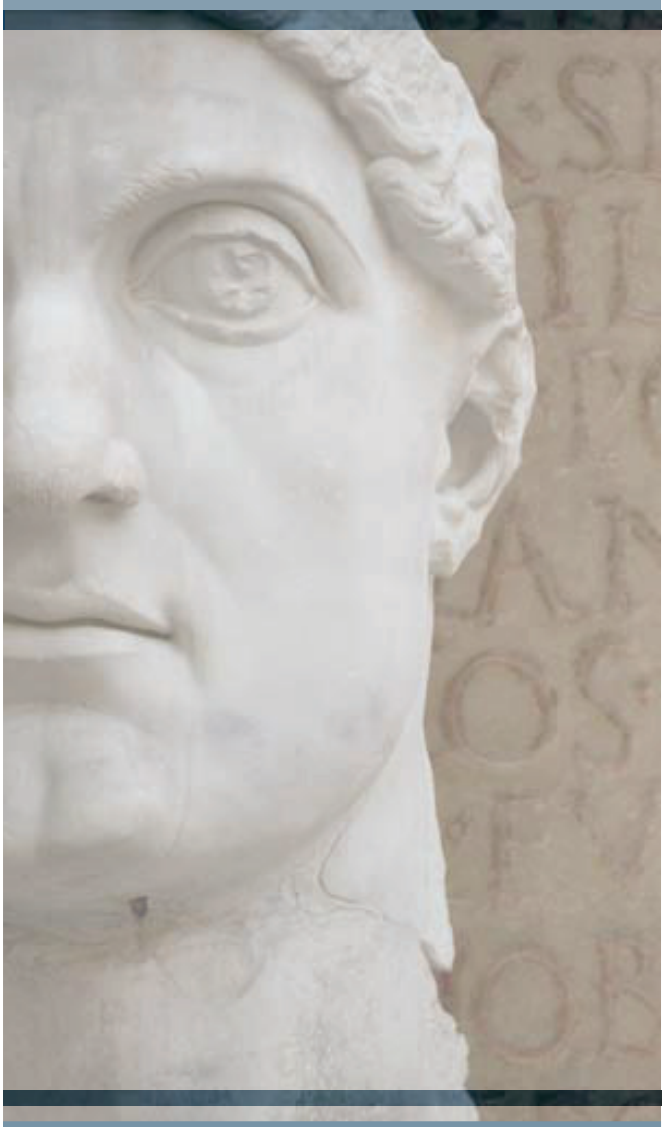
Defining with certainty when a cyber-attack to sensitive targets can be considered as a "violation", or when it can have the nature of a real "armed attack", represents a common priority by now, especially in a Western world which is interconnected and bases its entire social welfare on the functioning of information technologies.

The path was paved by the US Government[76], but an increased number of countries have started to modify their strategic philosophy, even providing for the launch of **offensive military operations via the cyber-space**[77]. The future of cyber-attacks will be a challenging one.

75. E. Nakashima, "U.S. accelerating cyberweapon research", in Washington Post, 2012, at http://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html.

76. David E. Sanger, Thom Shanker, "Broad Powers Seen for Obama in Cyberstrikes", 2013, at http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html. Department Of Defense, "Strategy for Operating in Cyberspace", 2011, at http://www.defense.gov/news/d20110714cyber.pdf.

77. As latest, Australian Government – Department of Defence, "Defence White Paper 2013", 2013, at http://www.defence.gov.au/WhitePaper2013/docs/WP_2013_web.pdf; Gouvernement Français, "Livre Blanc Sur la Défense et la SécuritéNationale 2013", 2013, at http://www.elysee.fr/assets/pdf/Livre-Blanc.pdf; United States Congress, National Defense Authorization Act For Fiscal Year 2012, "Military Activities in Cyberspace", Sec. 954, at http://www.fas.org/irp/congress/2011_cr/cyberwar.html.



ISTITUTO ITALIANO
DI STUDI STRATEGICI
ITALIAN INSTITUTE
OF STRATEGIC STUDIES
Niccolò Machiavelli

The Italian Institute of Strategic Studies "Niccolò Machiavelli" is a cultural non-profit organization founded in Rome in 2010.

The Institute, an independent think tank, was founded by the initiative of an international group of distinguished thinkers, academics and renowned professionals from civil and military institutions, with the aim of contributing to the renaissance of the Italian strategic thinking.

The complexity and scale of the challenges facing the nation in the twenty-first century requires knowledge, awareness and perspective capabilities. The Machiavelli Institute, thanks to its global network, promotes cultural exchange between Italian and international decision makers, from public and private sectors, and conducts researches with the aim of enhancing Italian global competitiveness.

The Machiavelli Institute, in cooperation with national and international institutions, organizations and corporate, produces studies and policy-oriented strategic analysis, organizes briefings, seminars and workshops, designs and delivers advanced courses for leaders.

For further information:

Italian Institute of Strategic Studies "Niccolò Machiavelli"
Via di S. Basilio, 64
00187 – Rome
Tel.: (+39) 06 45422952
Fax: (+39) 06 97259168
email: info@strategicstudies.it
www.strategicstudies.it