JOURNAL OF THE SPANISH INSTITUTE FOR STRATEGIC STUDIES

Manuel R. Torres Soriano

Full Professor, Political Science, Pablo de Olavide University, Seville.

E-mail: mrtorsor@upo.es

PROXY WARS IN CYBERSPACE

Abstract

This article proposes an in-depth study into the specific dynamics of cyberspace as a stage onto which to project so-called “proxy wars”. Its basic thesis is that the main advantage which this strategy provides (low risk of retaliation by the actor under attack) is also its principal weakness, since indirect participation in a cyber conflict detracts from a State’s efficiency in reaching tactical objectives, and is of only moderate value for advancing towards the achievement of strategic objectives. Throughout the paper, analysis is made of the advantages and limitations of this strategy, and a typology of the various cyber proxies is proposed based on their relation to the State utilizing them.

Keywords

Cyberspace, conflicts, espionage, deterrence, hacktivism.

PROXY WARS IN CYBERSPACE

INTRODUCTION

The possibility of furthering strategic interests at low cost has been a powerful incentive resulting, throughout history, in a number of States opting for so-called delegated wars, subsidiary wars, or—from the English—proxy wars. These have traditionally been understood as conflicts wherein a third party intervenes indirectly to influence the outcome in favor of that faction whose victory improves the relative power position of its sponsor. This strategy is an attractive option for countries seeking to avoid the high costs, in human and economic terms, implied by direct participation in an armed confrontation.

Recourse to proxy wars was especially prevalent within the strategic context of the Cold War, where the risks of nuclear escalation turned this option into the recourse of least risk for the weakening of the adversary's position. The end of hostilities between the Blocs did nothing to reduce the appeal of indirect confrontation. The British Professor Andrew Mumford[1] points to four factors which would have bestowed a renewed interest upon proxy wars:

a) The reticence of public opinion when support is needed for war as an instrument favoring the national interest.

b) The rise in importance and capabilities of private military companies (PMC's, in their English initials) which turns them into an actor on which to lean in order to indirectly project a State's resources of force.

c) The rise of China as a power, and the need to contain its influence without a direct confrontation and without prejudicing the existing economic interdependence.

d) The availability of cyberspace as a platform on which to participate indirectly in a conflict.

The purpose of this article is to provide an in-depth study into the specific dynamics possessed by cyberspace as a stage onto which to project the so-called proxy wars. The accumulation of cyber incidents of varying origin and nature throughout the past decade permits enjoyment of a body of evidence from which to sketch the first generalizations about the dynamics of performance of the actors who sponsor, or participate actively in, this type of conflict. The basic thesis is that the principal advantage provided by this strategy (low risk of reprisals by the actor under attack) is also its main weakness, since the indirect participation in a cyber conflict detracts

[1] MUMFORD, Andrew, "Proxy Warfare and the Future of Conflict", *The RUSI Journal*, vol. 158, no. 2 (2013), pp. 40-46.

from the efficiency of a State in reaching tactical objectives, and is of only limited value in achieving strategic objectives.

DISPROPORTIONATE EXPECTATIONS

Cyberspace as a stage for conflict gives an impression of being the quintessence of those characteristics which have made proxy wars the preferred option for such actors as a wish to promote their interests assuming a low level of risk. On the one hand, an initial assumption is made that this new technological environment creates a powerful incentive for the parties to resolve their difficulties through conflict. On the other, it is taken for granted that the anonymity and difficulty of attributing responsibility in the face of a cyber attack permit a high level of "plausible denial". It is usually assumed that there exists a low barrier of access to cyber conflict, due to the minimal economic cost represented by the development of cyber capacities. Similarly, the ubiquity and democratization of access to the new information technologies would have generated a vast number of actors on which to base the erosion of the adversary's position.

In spite of the fact that these views of the nature of cyberspace have solid roots in public opinion and the communication media, there is a need to take note of a number of qualifying aspects.

In the first place, in speaking of cyber attacks, an abusive use is made of the term as referring equally to actions as different in their technical viability and impact as are espionage, intellectual property theft, harassment, or the provoking of physical harm against persons or infrastructure through cyberspace.

While it is true that anonymity and secrecy are basic requisites to work in cyber espionage, for other types of action these may hold little or no strategic value[2]. For a State to undergo an attack which damages its economy, its infrastructure, or the life of its citizens, without knowing its origin, or the reason for which it was carried out, is of little coercive value. Absolute anonymity, in which it is not possible to establish even a speculative attribution as to motivation, may rather be a problem for the attacker than for the defender. Technology has not transformed the political nature of war once formulated by Clausewitz: an act of coercion directed towards an enemy (regardless of the instrument of projection) is still an action intended to bring about a modification in the behavior of the other actor according to the will of the first. The mere use of violence (physical or symbolic), if unaccompanied by an indication of why it was employed and what conditions will cause its cessation, is hardly likely to contribute to achieving the objectives of the attacker. Although it may be argued that one possible advantage of "anonymous violence" through cyberspace is that of

[2] BETZ, David, "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed", *Journal of Strategic Studies,* vol. 35, nº 5 (2012), pp. 689-711.

degrading the economy and power of an adversary[3], with no need to assume the cost of a reprisal, the fact is that in full globalization, the advanced degree of economic, commercial and financial interrelation means that any attempt to alter the balance of power by degrading the wealth, connectivity or the degree of confidence with which a competitor uses digital services, ends by generating consequences which are negative for the interests of the attacker. In this sense, economic cyber sabotage produces a negative-sum scenario in which all actors participating in the global economy in the end are injured, the only difference lying in which bears the greater damage.

As to the rise in conflict stemming from the availability of these new resources, the empirical evidence[4] shows how antagonists are willing to tolerate the existence of isolated cyber aggression as long as it does not go beyond the limit of what is considered an explicit act of war. In the numerous inter-State conflicts occurring in the past two decades, it may be observed how the predominant attitude between the actors who possess these capacities has been to recur only to very low-level operations, or to renounce their use, even in situations of open warfare. The risk of setting a precedent[5] which might encourage other competitors to follow the same route, together with fear of collateral damage, or the loss of control over its effects, have continued to condition the strategy of confrontation. This is the reason why, for example, the United States, despite considering their use, renounced their employment against the Iraqi banking system in 2003, or against the communication infrastructure of Colonel Gaddafi in 2011[6].

This attitude of restraint is also motivated by the operative nature of the so-called "cyber arms", many of which are single-use instruments, based on the exploitation of one or several vulnerabilities (of software as well as hardware), which remain unknown except to the actor who has discovered them and who has known how to make use of them. Unlike the majority of conventional arms, in the "cyber environment", the so-called "demonstration effect" does not apply, wherein a country is led to force the use of its new acquisitions in an armed conflict, or to show off its acquisition at public

[3] This is a view popular among many analysts who consider that actors such as China are immersed in a strategy against the U.S. they call "Death by a thousand cuts", where the risk to the North American country is not a great "Pearl Harbor style" attack, but rather the constant and silent action of theft of the intellectual property of its companies, which is intended to drain wealth and innovation from the country into its Chinese competitor. See: LINDSAY, JON R. and CHEUNG, Tai Ming, "From Exploitation to Innovation. Acquisition, Absorption, and Application" in LINDSAY, JON R., "China and Cybersecurity. Espionage, Strategy and Politics", T*he Digital Domain*, Oxford: Oxford University Press, 2015.

[4] VALERIANO, Brandon G. and MANESS. Ryan, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011", *Journal of Peace Research*, vol. 51, nº 3 (May 2014), pp. 347-360.

[5] LITWAK, Robert and KING, Meg, "Arms Control in Cyberspace?", *Wilson Briefs,* (October 2015). https://www.wilsoncenter.org/publication/arms-control-cyberspace.

[6] KAPLAN, Fred, "Dark Territory. The Secret History of Cyber War", New York, Simon and Schuster, 2016.

events, to thus strengthen its dissuasive character before potential enemies. On the contrary, the use of a cyber weapon reveals the advantage possessed by the actor using it, which causes the potential victims to correct those vulnerabilities and take active measures to avoid an identical cyber attack. This leads the antagonists to ration the use of their cyber arsenals, making use of them only in contexts where no other viable alternative exists, or even renouncing their present use so as to have them available in a potential conflict of greater importance.

This restraint may be observed even in actors with a greater predisposition for the use of force. It is highly significant that in the conflict between Russia and the Ukraine, hardly any major cyber attacks were produced beyond the usual attacks of denial of service and the sabotage of web pages on the part of patriotic cyber militias and hacker groups[7]. The Russian annexation of part of the Ukrainian territory and its attempt to destabilize the Kiev regime have been interpreted as a crystal-clear example of so-called "hybrid warfare", where the attacker makes intensive use of those resources of force which allow him to diffuse his responsibility during the development of the conflict. In spite of recourse to cyberspace fitting perfectly into the strategy of concealment, in the Russian case the fear of undesirable effects weighed more than the advantages its use could provide[8]. In the words of a member of U.S. intelligence, the problem with using a cyber weapon is that "once it's been revealed, it's the same as using an invisible airplane for the first time, you've rung the bell, and you can't maintain that the plane no longer exists. The question is: which aerial battle do you really want to use your invisible plane in?"[9]

One of the most established myths about cyber conflict is the supposed technical impossibility of establishing the origin of an attack, which would have spurred the aggression of a great number of actors sheltered by the anonymity provided by cyberspace. The reality is that although technically it is complex to determine the authorship of a cyber attack, it is not an impossible task[10]. In fact, the forensic aspect is not a determinant element; at times, it is not even the principal one. The reaction against the attacker follows a political logic[11], and as such, makes it unlikely that the aggressor will go unpunished due to lack of reliable proof of his guilt, as would

[7] LIBIKI, Martin, "The Cyber War that Wasn't", in GEERS, Kenneth (ed.)"Cyber War in Perspective: Russian Aggression against Ukraine", Tallin: NATO CCD COE Publications, 2015. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective full book.pdf.

[8] VALERIANO, Brandon G., and MANESS, Ryan, "Cyber wars versus Cyber Realities." "Cyber Conflict in the International System", Oxford: Oxford University Press, 2015.

[9] KETTER, Kim. "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon", Random House, New York, 2014.

[10] GUITTON, Clement and KORZAK, Elaine, "The Sophistication Criterion for Attribution: Identifying the Perpetrators of Cyber-Attacks", The RUSI Journal, vol. 158, nº 4 (2013), pp. 62-68.

[11] GOMPERT, David C. and LIBICKI, Martin, "Waging Cyber War the American Way", *Survival Global Politics and Strategy*, vol. 57, nº 4 (August-September 2015), pp. 7-28.

happen, for example, in a judicial process. It is very difficult for authorship to remain hidden when action takes place within a framework of pre-existing rivalry[12]. Thus, for example, it is logical, when South Korea finds itself under cyber-attack, to look to its neighbor to the north[13], or when Georgia and Ukraine undergo cyber-sabotage, that they should suspect Russia. Therefore it is very debatable whether the use of cyber warfare is an activity free from cost to the user because of the impossibility of attributing responsibility[14] .

Regarding the supposedly low cost of cyber attacks, this is a case of erroneous perception whose origin is located in extending to the military use of cyberspace the modus operandi of cybercrime, which is largely based on the use of automated tools, cheap and easily accessible, to carry out hundreds of thousands of attacks against computers and devices having low or deficient security. These are "scalable" attacks, where the cost of the operation does not increase linearly with the number of objectives attacked, which permits the indiscriminate use of malicious software to capture data from the victims, take control of their equipment, or simply cause involvement in a scam. However, in the case of attack on individualized objectives equipped with good protection, or with unique characteristics, the reference is to non-scalable attacks, which demand a supplementary force for each additional unit, as well as having available intelligence resources which provide extensive knowledge of their objective, and the capacity to test the vector of attack before their use[15].

Although the economic cost of cyber warfare is far below what a State would have to invest in acquiring a complex arms system, its cost is not negligible. In an exercise carried out by the United States in 2002, it was estimated that the carrying out of a major cyber attack would require a budget of 200 million dollars, as well as a period of five years for its implementation[16]. In spite of the popular imagery, the possibility of taking control and causing damage or anomalous behavior in critical infrastructure (as might be a nuclear plant), using only a computer connected to Internet, is an unreal scenario. The true entrance threshold is found in the capacity to mobilize objective-recognition resources, human and signal intelligence, the use of operatives on the ground, multidisciplinary teams of technicians and experts equipped with

[12] AXELROD, Robert, "A Repertory of Cyber Analogies", in GOLDMAN, Emily O. and ARQUILLA, John (eds.) "Cyber Analogies", Monterey, CA. Department of Defense Information Operations Center for Research, 2014.

[13] INKSTER, Nigel, "Cyber Attacks in La-La Land", *Survival: Global Politics and Strategy,* vol. 57, nº 1 (February-March 2015), pp. 105-116.

[14] RID, Thomas and BUCHANAN, Ben, "Attributing Cyber Attacks", *Journal of Strategic Studies,* vol. 38, nº 1-2 (2015), pp. 4-37.

[15] LINDSAY, John R., "Proxy Wars: Control Problems in Irregular Warfare and Cyber Operations", International Studies Association annual meeting, San Francisco (April 2013).

[16] PURCHASE, Eric and CALDWELL, French, "Digital Pearl Harbor: A Case Study in Industry Vulnerability to Cyber Attack" in GHOSH, Sumit, MALEK, Manu and STOHR, Edward A. (coord.), "Guarding Your Business: A Management Approach to Security." New York, Springer, 2004.

appropriate expertise, and the ability to evaluate the efficiency of the cyber weapon in a real environment, before proceeding to its use. This implies, therefore, requirements which go far beyond the mere availability of economic resources, and which surpass the capacities of many of the potential candidates for use as proxies in a cyber conflict.

WHAT CYBER PROXIES PROVIDE

In spite of the fact that expectations regarding the capacities of cyber proxies may be exaggerated, their contribution to a conflict is not negligible. An actor attempting to use this route to impose his interests will obtain four main benefits:

a) *Reduction in the risk of escalation.* A complex cyber attack requires previous reconnaissance activity regarding the networks and services towards which it is directed. The preparatory activities are indistinguishable, in an operational context, from those which have espionage as their sole purpose[17], which may produce an erroneous interpretation of the intentions of the party responsible for illegitimate access. This ambivalence is dangerous in an environment of elevated tension, since routine intelligence activities may be interpreted as an indication of imminent attack, giving rise to disproportionate response. Recourse to a proxy to carry out these tasks is an attractive option, since, should detection take place, the intrusion seems less serious than if its authors were organically linked to the institutional network of a State.

b) *Increased deterrent capacity.* One of the topics most debated with respect to the strategic implications of cyber warfare is the difficulty of implementing the classic theory of military deterrence[18]. Questions arise as to how to interpret the requirement for proportionality of response, when cyber objectives do not exist upon which to take reprisals; or when responding in kind presents a conflict of values. The availability of a proxy permits the State to augment its set of tools for reprisal, embracing as well those actions which it may not directly carry out due to moral or legal limitations. Its coercive power is reinforced when the utilization of a proxy permits tacit threats through acts which are found within the terrain of the illicit: "doxing" on key individuals, ex-filtration of intellectual property from its competitor's companies, scams, etc.

An example which illustrates the role proxies can play as agents of coercion may be found in the cyber attack undergone by the Sheldon Adelson casinos[19]. This

[17] LIN, Herbert, "Operational Considerations in Cyber Attack and Cyber Exploitation", in REVERON, Derek S., "Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World", Washington, D.C.: Georgetown University Press, 2012.

[18] LINDSAY, Jon R., "Tipping the scales: the attribution problem and the feasibility of deterrence against cyber attack", *Journal of Cyber security,* vol. 1, nº 1 (2015), pp. 53-67. http://cybersecurity.oxfordjournals.org/content/cybers/1/1/53.full.pdf.

[19] KAPLAN, Fred, "Dark Territory. The Secret History of Cyber War", New York: Simon and Schuster, 2016.

American millionaire holds an extensive history as a defender of the policies of the State of Israel. In a speech at a New York university he was asked his opinion about the nuclear agreement of the United States with Iran, to which Adelson responded: "*What I would say is this: Listen. See that desert out there? I want to show you something.*" Adelson stated that he would then drop a nuclear bomb. *"The explosion would harm no-one—maybe a couple of rattlesnakes, scorpions…whatever",* he continued. But he would give a warning: "Do you want to be eliminated? That's what I would say to those mullahs." The video went viral on Youtube. Two weeks later, Ayatollah AliKhameini, supreme leader of Iran, stated that the United States should *"slap those charlatans and crush their mouths".* A day after that statement, the web page of the chain of Las Vegas Sands casinos was hacked, by a collective calling itself Anti-WMD Team, so that it showed the following message: "Encouraging the use of Weapons of Mass Destruction UNDER ANY CONDITION is a crime." Parallel to this defacement[20] a cyber attack took place which destroyed twenty thousand computers within the casino's network, with an estimated cost of 40 million dollars. The authors of the attack also sent to the communications media a video showing the passwords for access to the casino network, and sensitive information about the company.

Within the environment of dictatorial regimes, these actors, especially if they are cloaked in the appearance of a "patriotic militia", may also be employed to carry out coercion of political dissidents and other groups against which it is preferred not to act explicitly because of the prejudice this may represent for the foreign image of these governments.

c) *Provide speed and flexibility*. The speed with which a State responds to cyber aggression which does not affect the basic pillars of its security is conditioned by the capacity to construct "a case" against those responsible for the attack. For this, it must not only collect technical and intelligence evidence so as to produce a solid attribution of responsibility, but must also make public opinion aware of the necessity for the response. This process is hindered if the aggressor has taken pains to dilute its responsibility by, for example, using a proxy in order to enjoy plausible denial.

In order to enjoy greater agility when constructing a response, States may encourage, actively or tacitly, the range of cyber proxies which sympathize with them to take reprisals against the sponsors of, or those responsible for, the aggression. Along these lines, the insistence in recent years on the so-called "active defense" of "cyber torsion"[21] is none other than a euphemism for the outsourcing to companies, and to other private actors of reprisal, of actions against the proxies used by other actors.

[20] *Defacement* is an English Word which may be translated as "to disfigure". This term is employed in the IT field to refer to the deformation or change produced intentionally on a web page by an attacker who has hacked into it.

[21] VALLEJO, Angel, "The advance in cyber torsion", Ciber Elcano, nº 3 (May 2015), pp. 7-13. http://www.realinstitutoelcano.org/wps/wcm/connect/68979900485661a5a4b6b77939ebc85f/Ciber Elcano Num3.pdf?MOD=APERES&CACHEID=1431364739259.

d) *Allows undercover operations.* Recourse may be had to a proxy in order to avoid the barriers hindering a State from acting explicitly in specific environments of cyberspace. One of the most meaningful examples is that of the black markets in *exploits*. The cyber capacities of an actor are directly linked to his ability to construct an arsenal of hardware and software vulnerabilities which may be integrated into his operations in cyberspace. Although the most advanced actors are capable of detecting and deactivating these breeches of security by their own means, normally they also have recourse to non-regulated markets for the sale and purchase of *exploits* to increase their resources[22]. The direct intervention by a State agency on these non-regulated, or illicit, markets presents a series of problems which may be avoided if this intervention is carried out undercover. So, for example, a legal dilemma exists the moment a State has acquired (usually using opaque funds[23]) a vulnerability which compromises not only the security and secrecy of its adversary's communications, but also that of citizens themselves. In spite of this, it decides not to make public this vulnerability to avoid its being "patched", and to exploit to its benefit this ignorance. Using a proxy as intermediate actor offers not only denial capability but also additional advantages such as the avoidance of an image crisis when the existence of the interactions with actors of dubious reputation is exposed[24], or keeping adversaries from being able to create an accurate image of the cyber capacities which the State has at is disposition.

A TYPOLOGY OF CYBER PROXIES

The nature of the link established between a State and those groups which it uses as proxies in a cyber conflict is an essential element in order to understand its dynamics of performance and capacities. Therefore, the following typology is suggested:

[22] HARRIS, Shane, "@War. The Rise of the Military-Internet Complex", Boston, Mariner Books, 2015.

[23] DIEBERT, Ronald J., "Black Code: Inside the Battle for Cyberspace", Toronto, Signal/McClelland & Stewart, 2013.

[24] This was the situation which was produced when the controversial Italian company Hacking Team, dedicated to the sale of software for the offensive monitoring of communications systems, underwent hacking which resulted in the publication on Internet of 400 gigabytes of company data, including its list of clients and contracts. Many democratic governments had to contend in the face of their country's public opinion with the inconvenient reality of having done business with a company which had on its list of purchasers certain dictatorial regimes which used its services to repress opposition and violate human rights. See: KOPSTEIN, Joshua, "Meet the Companies that Helped Hacking Team Sell Tools to Repressive Governments", *Mother Board* (July 2015). https://motherboard.vice.com/read/meet-the-companies-that-helped-hacking-team-sell-tools-to-repressive-governments.

a) *Captive proxies*. Refers to those actors whose link is one of a solid legal or economic dependence on one or several States, which confers on the latter a clear power to orient their actions towards specific objectives, or to stop them from acting towards others. The paradigmatic example of these actors may be seen in cyber security companies. The militarization of cyberspace has forced a transformation in the environment in which these companies carry out their services. In a short time, they have changed from a business model whose nearly exclusive objective was to offer security solutions to private, company and State customers facing use of malicious software developed by individual and groups for criminal profit, to a new context where State actors are the most important creators and users of this type of code. A cyber security staff member of the American company Adobe stated in 2011 that the adversaries who really worried him were the "airplane-carrier" types: those with enough money to acquire the major exploits found in its programs, and the expertise necessary for their use[25].

In recent years, cyber security companies have been key to the revelation of the existence and supposed authorship of some of the principal offensive actions in cyberspace. In doing so, these companies have had to face the ethical and political dilemma as to which loyalty should take precedence: that towards their potential clients, or towards the national interests of the countries which shelter them.

These companies may become proxies by omission, where the demand of the State is that they restrain activities of investigating or publicizing the authorship of certain operations where such activities might put at risk the viability and success of these cyber operations.

These private actors may carry out a more active role when carrying out their activities in contexts where "State capitalism" is practiced, or where it is impossible to operate without the approval of the country's rulers (e.g. China, Russia and Iran). States can profit from the credibility associated with certain brands, sponsoring their action towards certain objectives, transferring knowledge, offering technical assistance, or providing intelligence resources so that they may be successful when actively sabotaging the intelligence operations of their adversaries, or weakening their international image.

The seeming freedom of these companies becomes the screen permitting implementation of a proactive strategy. Thus, for example, the Russian company Kaspersky has been perceived "not only as an anti-virus company, but as the leader in exposing cyber espionage[26], due to its chief role in revealing the existence of two of the most important cyber operations of the United States to date: Stuznet and Flame. For some observers, the background of its founder, Eugene Kaspersky, as a member of the intelligence service of the USSR, and the constant interference

[25] ZETTER, Kim, "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, New York: Crown, 2014.

[26] SHACHTMAN, Noah, "Russian's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals", *Wired* (June 23, 2012), http://www.wired.com/dangerroom/2012/07/ff Kaspersky/.

of the Russian State with several economic agents, far from being irrelevant data, represent evidence about the geostrategic utilization which some of the principal companies in the sector undergo. The pressure exerted by governments on the commercial sector may also be carried out by more subtle means, especially when they find themselves limited by the State of Law and democratic referendum. The state actors exploit to their benefit the commercial competition existing among the companies in the sector, as well as their need to add a differential element to their services. The value of these companies, on too many occasions, is related more to the alarm existing among their potential clients and their own ability to elaborate showy reports than to the quality of their products and their capacity to provide solutions to specific problems. A fierce competition has arisen in recent years to expose new cases of APT's[27] (jokes are made within the industry about "Advanced Persistent Marketing). This leads companies to precipitate their conclusions based solely on circumstantial evidence. These companies usually demonstrate their principal strengths in the forensic analysis of the malware detected. However, basing identification of a recurrent APT exclusively on this type of information constitutes an enormous limitation, since this evidence may be ambiguous or deliberately misleading.

A good many of the reports prepared by these companies seek a broad media impact using titles inspired by popular imagery of the functioning of an intelligence service. For this, they imitate supposed keyed codes to designate the new operations which they believe they have discovered. However, it is not unlikely that several of these products are referring to the same perpetrators but with different names[28], that these actors do not exist as organizations with their own identity, or that their components have fluctuated from group to group without our knowing this.

The proper way to deal with this kind of slant is to confront and complement these conclusions with data proceeding from other sources of intelligence (especially human). However, it is in this other dimension of analysis where these companies demonstrate their principal failings[29]. States can take advantage of this need in order to orient, through informal filters or collaboration, the work of these companies towards the objectives it is desired to act upon. These informal channels may be fundamental for the progressive generation of a climate of opinion which strengthens the position of the country in the face of its adversaries.

[27] "Advanced Persistent Threats", (APT's in the English abbreviation) are understood to refer to a complex operation of cybernetic infiltration directed against specific objectives over time, and which, unlike automated actions, have a major human component, in the design as well as in the implementation of the action.

[28] SCOTT, James and SPANIEL, Drew, "Know Your Enemies 2.0", *ICIT Report,* (February 2016). http://icitech.org/wp-content/uploads/2016/02/ICIT-Brief-Know-Your-Enemies-2.0.pdf.

[29] LEE, Robert M. and RID, Thomas, "OMG Cyber!", *The RUSI Journal*, vol. 159, nº 5 (October-November 2014), pp. 4-12. http://www.tandfonline.com/doi/pdf/10.1080/03071847.2014.969932.

b) Dependent proxies. These lack autonomy with respect to the State which creates and utilizes them. This is the case, for example, of the relationship established between the regime of Bashar al-Assad and the so-called Syrian Electronic Army (SEA), to which there has been attributed a large number of cyber-sabotage actions towards international communications media and opposition groups which demonstrate hostility to the Syrian dictator.

On occasions, these proxies are not only ad hoc creations, but the State also shows little interest in demonstrating possession of an entity of its own which goes beyond the operation for which it was created. Such is the case with the self-styled "Cutting Sword of Justice", which defined itself as "a group of anti-oppression hackers" claiming responsibility in the summer of 2012 for the cyber attack on the computer network of the Saudi petroleum company Aramco, damaging over 30,000 of the company's computers. This supposed group lacks any previous record or public profile. Its only manifesto was limited to a brief written communiqué on the website of the Pastebin anonymous publications, where it justified its actions as a response to the "crimes and atrocities taking place in a number of countries throughout the world, especially in neighboring countries such as Syria, Bahrein, Yemen, Lebanon, Egypt…", which were sponsored, according to the communiqué, using the oil resources of the Moslems[30]. Speculations about the origin of the attack were soon directed towards Iran[31], something which that country probably desired, considering its indifference to the continuity in time of "Cutting Sword". Iran had already undergone, at the hands of the United States and Israel, the greatest cyber attack known up to that moment (Stuxnet), and wished to make a public display of its new cyber warfare capacities by directing an action against its principal regional rival and ally of its enemy, the United States. Through a one-time action, attributed to an apparently independent proxy, and oriented towards a company (and not a political institution or military facility), the Persian country indirectly reinforced its capacity for cyber dissuasion, so avoiding the risk of a military response by the Saudi kingdom.

Within this same category are included as well those proxies which demonstrate a more obvious organic link to their sponsors. This is the case of the so-called Iranian Cyber Army, a creation of the Iranian Revolutionary Guard (IRGC in its English abbreviation)[32] which is used against objectives for which there is no major need to disseminate responsibility, either because an overt and active hostility exists though other routes (as is the case with Israel), or because there is

[30] MCKIE, Gladys, "Cutting Sword of Justice", Cyber Threat Research (no date). https://cyberthreatresearch.wordpress.com/hackivist-groups/cutting-sword-of-justice/.

[31] BRONK, Christopher and TIKK-RINGAS, Eneken, "The Cyber Attack on Saudi Aramco", *Survival*, vol. 55, nº 2 (April 2013), pp. 81-96.

[32] ADELKAH, Nima, "Iran and Its Cyber Terrorism Strategies", *Terrorism Monitor*, vol. 14, nº 10 (May 16, 2016). http://www.jamestown.org/single/?txttnews[ttnews]=45435&txttnews[backpjd]=7&cHash=fa0da141d630521600aa6a7bffa11625.

no fear of additional reprisals on the part of the victim (as in the case of the cyber operations against the terrorist group Islamic State.

c) *Tacit proxies*. This encompasses those actors whose survival depends on a tacit non-aggression agreement on the part of the State in whose territory is members are located[33]. Such is the case of the organizations dedicated to cyber crime. The existence of a vibrant transnational cyber delinquent sector may serve to reinforce strength when subcontracting cyber operations. In the case of Russia, for example, there exists a fluid interaction with these actors, which is favored by the criminal ties appreciable at the highest levels of government[34].

This type of sponsorship may also be carried out implicitly, without the need to produce direct channels of coordination. They are taken for granted where there exists a mutual understanding, according to which the actor who performs as proxy assumes that its actions are tolerated by the State from which the group operates, as long as the group limits its objectives to the prejudicing or erosion of the economic position of its adversaries, and abstains from extending its illicit activities to the domestic environment. A symbiotic relationship is produced between the group which is enriched through such activities as bank fraud, online scams, intellectual property piracy, etc., and the State, which tolerates this delinquent behavior because it degrades the economic strength of its adversaries, at the same time that it drains their wealth into its domestic economy, which finds itself stimulated by the circulation of money obtained fraudulently in other countries. It is a case of a re-editing 2.0 of the letters of marque used in the 18th and 19th centuries, with the difference that the State, far from recognizing this collaboration with the virtual pirates, publically manifests its determination to fight against cyber delinquency wherever it takes place.

d) *Autonomic proxies*. This term encompasses those actors who have an established identity of their own and an agenda which does not coincide exactly with the interests of the potential sponsor States. These are usually groups whose existence is not limited to the cybernetic environment, but who rather see the latter as just one of the manifestations of the group's activism, which may include the use of physical violence. An example of a group from this category is the Lebanese organization Hezbollah, which possesses considerable offensive capacities within the cybernetic environment, acquired in great measure through the proliferation carried out by Iran in order for this militia to harass Israel and the enemies of Iran's Syrian ally[35]. This type of actor is the one posing the most problems for the State attempting to utilize it, since the existence of an agenda of its own causes

[33] BORGHARD, Erica D. and LONERGAN, Shawn W., "Can States Calculate the Risks of Using Cyber Proxies?", *Orbis*, vol. 60, nº 3 (2016), pp. 395-416.

[34] SMITH, David, "Russian Cyber Operations", *Potomac Institute for Policy Studies* (2012). http://www.potomacinstitute.org/80-potomac-institute-cyber-center/piccpublications/670-new-picc-paper-russian-cyber-operations.

[35] JONES, Sam, "Cyber warfare: Iran opens a new front", Financial Times (April 26, 2016). http://www.ft.com/cms/s/0/15e1acf0-0a47-11e6-b0f1-61f222853ff3.html.

relations with its benefactor to evolve throughout a conflict, especially when the proxy is jealous of its autonomy and has a different outlook as to how it should advance towards its objectives.

PROBLEMS OF DELEGATION

Although delegation upon other actors permits the State sponsor to elude a part of any reprisals, it also reduces the effectiveness of the action of proxies, since their capacity for coercion cannot benefit from the direct and explicit involvement of their benefactor. Cyber conflict is in any case a manifestation of the exertion of the power of the State, which maintains the political objective of forcing another actor to do, or cease doing[36], something along the lines of its own interests. Cyber attacks maintain this political nature, and as such, the final aim is to coerce both the adversary and potential contenders. Nonetheless, the more a disconnection (real or simulated) is assumed to exist between a proxy and a State, the less its coercive power, since the only tools at its disposition to break the will of the victim are those which it has revealed with its cyber attack, as it has no recourse to the threat of an escalation employing the resources available to its sponsor.

This was the case with the so-called *"Comodo Hack"*, wherein a "patriotic Iranian hacker" claimed to have gained control over the digital certificates administered by authorization from *Comodo* Certifications, and which are used to authenticate such popular electronic mail services as Google Gmail, Yahoo Mail, or Microsoft Hotmail. This appropriation had supposedly given him the capacity to spy within these mails "the same as do the United States and Israel." The author of this attack took it upon himself through a communiqué to manifest the political nature of this action, accusing Western governments and companies of conspiring to spy upon and cyber attack his country. Referring to the so-called Green Movement and the terrorist group Organization of the Mujahaddins of the People (MKO in its English abbreviation), he stated that: "I am not going to permit anyone within Iran to harm the Iranian people, injure the nuclear scientists of my country, injure my leader (…) for these people, there is no privacy on Internet, they have no security in the digital world"[37]. Nonetheless, within the communiqué itself he underlined the individual nature of this action, stating that it was a question of a "21-year-old programmer" with no links to any group. His emphasis on the individual character of this attack detracted from the forcefulness of his threats, as is shown by the fact that this action has produced no modification in the behavior of his recipients.

[36] BETZ, David and STEVENS, Tim, "Power and cyberspace", *Adelphi Series*, Vol. 51, nº 424 (2011), pp. 9-34.

[37] BRIGHT, Peter, "Independent Iranian Hacker Claims Responsibility for *Comodo Hack*", *Wired* (March 28 2011). http./www.wired.com/threatlevel/2011/03/comodo hack.

Even when a cyber attack is used as a tool of pressure for the achievement of very specific objectives, and the presumption of State backing is high neither does this necessarily guarantee success. This is the case of the incident undergone by the cinema producer Sony during the Christmas holidays in 2014, when it was the victim of blackmail to avoid the public distribution of the comedy "The Interview". The tape, which parodies the North Korean President, had been defined by the spokesman of the Foreign Ministry of that country as "an actor of terrorism", announcing "merciless reprisals"[38] if the film was shown.

Some weeks before its showing in movie theaters, Sony underwent a cyber attack consisting of the theft of the electronic correspondence of all of its employees, as well as the appropriation of the copy of five unreleased or recently premiered films. All of this information was leaked to Internet, occasioning financial damage to the company from the illegal distribution of the tapes valued at 17 million dollars[39] as well as damage to the reputation of the company from the content of some of these emails showing the use of denigrating expressions about actors and other members of the American audiovisual community.

Responsibility for the theft of data was claimed by a group calling itself "Guardians of Peace", which took its threats beyond the cybernetic environment, announcing assaults on movie theaters projecting the film. The premier of the film was cancelled by the company, which caused major ill feeling, not only among actors who denounced the example Sony was setting in the face of blackmail, but even involving President Obama, who regretted that the demands of the attackers were being met. The company reconsidered its initial decision, and decided to project the film in a lesser number of "selected" theaters as well as to distribute it simultaneously on Internet.

As the final result of this episode, the film was not only released, but possibly achieved a wider audience than was originally foreseen due to the heightened public interest generated by this controversial production, which had been capable of infuriating the dictator. North Korea had no major interest in disassociating itself from this action, and yet it was generally assumed that North Korea would not in the last instance carry out the threats launched by the "Guardians", since this would suppose forcing an act of war against the United States.

Another of the problems with cyber conflicts by delegation are the risks associated with the selection and control of the proxies. The preferences of the latter may vary notably with respect to the sponsor. Some of them become disloyal as time goes by, and others are from the outset. The academic literature[40] points out, for example,

[38] BBC. "The interview: A guide to the cyber attack on Hollywood", *BBC News* (December 29, 2014).

http://www.bbc.com/news/entertainment-arts-30512032.

[39] RUSHE, Dominic, "The Interview revenge hack cost Sony just $15m", *the Guardian* (February 4, 2015), http://www.theguardian.com/film/2015/feb/04/guardians-peace-revenge-hack-sony-finances-unscathed.

[40] POPOVIC, Milos (2015), "Fragile proxies: Explaining rebel defection against their state sponsors", *Terrorism and Political Violence*, (2015) DOI: 10.1080/09546553.2015.1092437.

that control over these actors is made enormously more difficult if the State lacks the effective capacity to punish the transgressions of its partners, or if the latter possess a decentralized structure which does not guarantee correct compliance with the orders emanating from its leaders.

In addition, other peculiarities are to be found in the cyber environment. These actors perform on occasion in areas which the sponsor cannot, or does not wish to, reach into, which presents the problem of how to monitor their actions in an environment which remains opaque with regard to State control. The correct selection of these operatives is made difficult by the limitations existing when it is desired to check their backgrounds and trustworthiness, given that one of the characteristics making them useful is precisely their capacity to operate clandestinely.

The risk of a poor choice also lies in the inability to verify whether the proxy has the skill necessary to crown with success the mission he has been charged with. An incompetent "partner" may compromise the alibi of his sponsor, especially if the viability of the operation depends on the surprise factor, or on the ability to carry it without leaving an incriminating trail. This poor-quality work may even be found within the institutional setting, from which a higher level of professionalism is expected. Thus, for example, the cyber security company Madiant[41] was able to attribute to the Chinese army unit designated 61398 the responsibility for cyber espionage on 141 organizations throughout the world, based on the deficient operative security practices employed by the Chinese hackers. In the preparation and implementation of the operation they not only used test servers located within their own country, and Chinese IP sites, telephone numbers and keyboards, but also communicated with each other using colloquial Chinese expressions, and re-used their personal pseudonyms, which had been used in the past to participate in Internet forums, employment pages, etc., where photographs and identifying data of their owners were provided.

Another frequent error by an incompetent cyber proxy consists in the use of prematurely developed code, which usually produces errors causing failure when it is employed in a real context, or which generates undesired or counterproductive effects. There also exists the risk of causing "collateral casualties", extending the conflict towards other actors or prejudicing the image of the sponsor.

CONCLUSIONS

A simple review of the different episodes of delegated conflict in cyberspace demonstrates the limited efficacy of this strategy for the achievement of strategic objectives. The principal attraction of recurrence to a proxy (obtaining plausible

[41] MADIANT. "APT 1: Exposing One of China's Cyber Espionage Units", Mandiant Intelligence Center (2013). http://intelreport.mandiant.com/Mandiant APT1 Report.pdf.

negation upon assaulting an enemy) is also its principal weakness. The lack of State backing dilutes to a great degree the coercive power which this type of action could hold.

Cyber proxies clearly show their usefulness when they are employed in operational contexts where there exists an undeniable need to obscure State authorship, as for example acts of obviously criminal nature or of espionage.

Despite the fact that the deeds of this type of actor have taken place at the most technically superficial levels of what is called cyber warfare, it is premature to state that these proxies are destined to perform a marginal role in forthcoming cyber conflicts. Although in the last decade exponential growth has taken place in the number of cyber incidents related to State rivalries, we still find ourselves within an experimental context wherein States have not fully matured their doctrines of performance within this new technological scenario. Many of these incidents are of an exploratory character, where through a process of trial and error, States learn about the effects of the employment of these resources and the responses of the State's adversaries, as well as the potential integration of such resources into offensives going beyond the virtual environment.

In the same way, neither should it be discounted that much of this low-level conflict has as its objective the creation of operative expertise and a credibility rating for the proxies themselves, which to date have been less than efficacious due to the lack of these guarantees. The fact that these groups maintain a level of activity apparently unconnected with the interests of any country contributes to reinforce the alibi which the State counts on when deciding to align them in its favor. In an environment of great uncertainty, these actors permit certain States to enter the environment of cyber warfare to survey its possibilities without excessive risk. In this sense, proxies may assume the function of initiating and sustaining cyber conflicts of low intensity which will in future be absorbed and enhanced by the intrinsic capacities of the State in a context which they find more favorable.

BIBLIOGRAPHY

ADELKHAH, Nima. "Iran and Its Cyber-Terrorism Strategies", *Terrorism Monitor,* Vol. 14, No. 10 (May 16, 2016) http://www.jamestown.org/single/?tx_ttnews[tt_news]=45435&tx_ttnews[backPid]=7&cHash=fa0da141d63052f600aa6a7bffa1f625.

BBC. "The Interview: A guide to the cyber attack on Hollywood", *BBC News* (December 29, 2014). http://www.bbc.com/news/entertainment-arts-30512032.

BETZ, David and STEVENS, Tim. "Power and cyberspace", *Adelphi Series*, Vol. 51, No. 424 (2011), pp. 9-34.

BETZ, David. "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed", *Journal of Strategic Studies*, Vol. 35, No. 5 (2012), pp. 689-711.

BORGHARD, Erica D. and LONERGAN, Shawn W. “Can States Calculate the Risks of Using Cyber Proxies?”, *Orbis*, Vol. 60, No, 3 (2016), pp. 395-416.

BRIGHT, Peter. “Independent Iranian Hacker Claims Responsibility for Comodo Hack”, *Wired* (March 28, 2011). http://www.wired.com/threatlevel/2011/03/comodo_hack/.

BRONK, Christopher yTIKK-RINGAS, Eneken. “The Cyber Attack on Saudi Aramco”, *Survival*, Vol. 55, No. 2 (April 2013), pp. 81-96.

DEIBERT, Ronald J. Black Code: Inside the Battle for Cyberspace, Toronto: Signal/McClelland & Stewart, 2013.

GEERS, Kenneth (ed.) Cyber War in Perspective: Russian Aggression against Ukraine, Tallin*:* NATO CCD COE Publications, 2015. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf.

GHOSH, Sumit, MALEK, Manu and STOHR, Edward A. (coord.) Guarding Your Business: A Management Approach to Security, Nueva York: Springer, 2004.

GOLDMAN, Emily O. and ARQUILLA, John (eds.) Cyber Analogies, Monterey, CA: Department of Defense Information Operations Center for Research, 2014.

GOMPERT, David C. and LIBICKI, Martin. Waging Cyber War the American Way, *Survival: Global Politics and Strategy, Vol. 57, No. 4 (*August–September *2015), pp. 7-28.*

GUITTON, Clement and KORZAK, Elaine. “The Sophistication Criterion for Attribution: Identifying the Perpetrators of Cyber-Attacks”, *The RUSI Journal*, Vol. 158, No. 4 (2013), pp. 62-68.

HARRIS, Shane. @WAR: The Rise of the Military-Internet Complex, Boston: Mariner Books, 2015.

INKSTER, Nigel. “Cyber Attacks in La-La Land”, *Survival: Global Politics and Strategy, Vol. 57, No. 1 (*February–March 2015), pp. 105-116.

JONES, Sam. “Cyber warfare: Iran opens a new front”, *Financial Times* (April 26, 2016). http://www.ft.com/cms/s/0/15e1acf0-0a47-11e6-b0f1-61f222853ff3.html.

KAPLAN, Fred. Dark Territory. The Secret History of Cyber War, New York: Simon & Schuster, 2016.

KETTER, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon, Random House, New York, 2014.

KOPSTEIN, Joshua. “Meet the Companies that Helped Hacking Team Sell Tools to Repressive Governments”, *Mother Board*, (July 9, 2015). https://motherboard.vice.com/read/meet-the-companies-that-helped-hacking-team-sell-tools-to-repressive-governments.

LEE, Robert M. and RID, Thomas. “OMG Cyber!”, *The RUSI Journal*, Vol. 159, No. 5 (October-November 2014), pp. 4-12. http://www.tandfonline.com/doi/pdf/10.1080/03071847.2014.969932.

LINDSAY, Jon R. "Proxy Wars: Control Problems in Irregular Warfare and Cyber Operations", International Studies Association annual meeting, San Francisco, (April 2013). http://www.jonrlindsay.com/papers.

LINDSAY, Jon R. "Tipping the scales: the attribution problem and the feasibility of deterrence against cyber attack", *Journal of Cybersecurity*, Vol. 1, No. 1 (2015), pp. 53-67. http://cybersecurity.oxfordjournals.org/content/cybers/1/1/53.full.pdf.

LINDSAY, JON R. China and Cybersecurity. Espionage, Strategy, and Politics the Digital Domain, Oxford: Oxford University Press, 2015.

LITWAK, Robert and KING, Meg. "Arms Control in Cyberspace?" *Wilson Briefs*, (October 2015). https://www.wilsoncenter.org/publication/arms-control-cyberspace.

MADIANT. "APT1: Exposing One of China's Cyber Espionage Units", Mandiant Intelligence Center (2013). http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

MCKIE, Gladys. "Cutting Sword of Justice", Cyber Threat Research (April 2014). https://cyberthreatresearch.wordpress.com/hacktivist-groups/cutting-sword-of-justice/.

MUMFORD, Andrew. "Proxy Warfare and the Future of Conflict", *The RUSI Journal*, Vol. 158, No. 2 (2013), pp. 40-46.

REVERON, Derek S. Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, Washington D.C.: Georgetown University Press, 2012.

RID, Thomas and BUCHANAN, Ben. "Attributing Cyber Attacks", *Journal of Strategic Studies*, Vol. 38, No. 1-2 (2015), pp. 4-37.

RUSHE, Dominic. "The Interview revenge hack cost Sony just $15m", *The Guardian* (February 4, 2015) http://www.theguardian.com/film/2015/feb/04/guardians-peace-revenge-hack-sony-finances-unscathed.

SCOTT, James and SPANIEL, Drew. "Know Your Enemies 2.0", *ICIT Report* (February 2016). http://icitech.org/wp-content/uploads/2016/02/ICIT-Brief-Know-Your-Enemies-2.0.pdf.

SHACHTMAN, Noah. "Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals", *Wired*, (June 23, 2012). http://www.wired.com/dangerroom/2012/07/ff_kaspersky/.

SMITH, David. "Russian Cyber Operations", *Poto Institute for Policy Studies* (2012). http://www.potomacinstitute.org/80-potomac-institute-cyber-center/piccpublications/670-new-picc-paper-russian-cyber-operations.

VALERIANO, Brandon G. and MANESS, Ryan. "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011", *Journal of Peace Research,* Vol. 51, No. 3 (May 2014), pp. 347-360.

VALERIANO, Brandon G. and MANESS, Ryan. Cyberwars versus Cyber Realities. Cyber Conflict in the International System, Oxford: Oxford University Press, 2015.

VALLEJO, Ángel. “El avance de la ciber-retorsión”, Ciber Elcano, No. 3 (May 2015), pp.7-13. http://www.realinstitutoelcano.org/wps/wcm/connect/6897990048566 1a5a4b6b77939ebc85f/Ciber_Elcano_Num3.pdf?MOD=AJPERES&CACHEID=1431364739259.

ZETTER, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon, New York: Crown, 2014.

Submited: September 5, 2016.
Accepted: December 19, 2016.