Revista de Pensamiento Estratégico y Seguridad CISDE

Recibido: 07-03-2017 / Revisado: 18-04-2017
Aceptado: 19-04-2017 / Publicado: 30-05-2017

CISDE Journal, 2(2), 2017

Cyberspace and European security

El ciberespacio y la seguridad europea

Joaquín Alfaro Pérez[1]; Inmaculada de Jesús Arboleda Guirao[2]

[1] Alférez del ejército del aire español. Base Aérea de San Javier, España
[2] Centro universitario de la Defensa. Base Aérea de San Javier, España

jalfpe2@mde.es , inma.arboleda@cud.upct.es

ABSTRACT. Nowadays, cyberspace constitutes one of the major channels for satisfying the needs, rights and interests of EU citizens. Throughout the last decade, cybersecurity incidents have increased at a frantic pace, thus becoming an important threat to the supply of basic services and affecting the economy of EU Member States. The majority of analysts and military specialists point out that life in the twenty-first century will comprise cyberattacks. Consequently, from the EU and the CSDP, we must give cyberspace the scope it deserves as the fifth warfare domain, equal to the four traditional ones of land, sea, air and space. The recruitment and training of the necessary skilled human capital, the strengthening of cooperation at all levels in cyberdefence issues and the development of a joint thinking or cyber-mindednes constitute the basis to achieve and maintain effective cybercapabilities among the Member States.

RESUMEN. Actualmente el ciberespacio constituye uno de los principales canales para satisfacer las necesidades, derechos e intereses de los ciudadanos de la UE. A lo largo de la última década, han aumentado a un ritmo vertiginoso los incidentes relacionados con la ciberseguridad, convirtiéndose en una grave amenaza para el abastecimiento de servicios básicos y afectando a la economía de los Estados Miembros de la UE. La mayoría de los analistas y especialistas militares señalan que la vida en el siglo XXI incluirá ciber-ataques. Por tanto, desde la UE y la PCSD, debemos dar al ciberespacio la dimensión que se merece como el quinto dominio bélico, similar a los cuatro tradicionales de tierra, mar, aire y espacio. El reclutamiento y la formación del necesario capital humano, el fortalecimiento de la cooperación en cuestiones de ciberdefensa y el desarrollo de un enfoque conjunto constituyen la base para alcanzar y mantener ciber-competencias efectivas entre los Estados Miembros.

KEYWORDS: Ciberespacio, PCSD, Ciberseguridad, Ciberataque, Ciberdefensa, Estados miembros de la UE.

PALABRAS CLAVE: Cyberspace, CSDP, Cybersecurity, Cyberattack, Cyberdefence, EU Member States.

Alfaro, J.; Arboleda, I. D. J. (2017). Cyberspace and European security. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 2(2), 71-78.

1. Introducción

Prior to World War I, the use of aircrafts was considered to be highly limited and very few people regarded them as a feasible military option. However, the next years saw the development of strategic-bombing aircraft and their application in significant military operations. At that time, theorists and military officers, like Giulio Douhet, Hugh Trenchard or William "Billy" Mitchell, guided the appearance of airpower as an important military tool (Lee, 2013).

Nowadays, as it happened with airpower in the early years of the aerial domain, there are those who still look at cyber power with some degree of skepticism.

For this reason it is necessary to raise awareness about the importance of giving cyberspace the scope it deserves as the fifth warfare domain. In Machiavelli´s own words (1515, p. 5): "And it ought to be remembered that there is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things".

When the European Council adopted the European Security Strategy (ESS) in December 2003, which established principles and set clear objectives in order to advance the European Union (EU)´s security interests, cyber incidents were not within the issues identified as key threats and global challenges. However,the rapid growth of the digital world has brought not only enormous benefits but also vulnerabilities. Consequently, in December 2008, five years after adopting the ESS, the High Representative´s (HR) Report on the Implementation of the ESS: Providing Security in a Changing World (European Parliament, 2015), recognised cybercrime as a potential new economic, political and military weapon.

Nowadays, cyberspace constitutes one of the major channels for satisfying the needs, rights and interests of EU citizens and Member States, providing an essential means for economic growth in the EU (Council of the EU, 2013) Moreover, Information and Communication technology (ICT) has become a critical resource which all economic sectors rely on. At the same time, cybersecurity incidents are increasing at a frenetic pace, thus becoming an important threat to the supply of basic services and affecting the economy of EU Member States. Therefore, governments have begun to develop cybersecurity strategies. In 2013 European Commission outlined the EU´s vision and the actions required to make the EU´s online environment the safest in the world (European Commission, 2013).

In December 2013, "the EU heads of state and government recognised cyber defence as a priority for capability development at the EU Council on defence matters" (European Council, 2013, p. 11). One of the five strategic priorities articulated in theCybersecurity Strategy of the EU is the development of cyberdefence capabilities and policy related to the Common Security and Defence Policy (CSDP). This document presents the actions required in the field of CSDP to increase the resilience of ICT systems supporting Member States´ defence and national security interests. The promotion of the development of EU cyberdefence capabilities is among the key activities pointed by the High Representative (HR) to focus on, inviting the Member States and the European Defence Agency to collaborate. Doctrine, leadership, organisation, personnel, training, infrastructure, technology, logistics and interoperability are some of the aspects covered within the capability development, thus providing a comprehensive approach which starts to outline cyberspace as the fifth operational domain at the same level of the first four war-fighting domains (land, sea, air and space).

2. Current state of research and research gap

Cyberspace is in a stage of development similar to the years between World War I and World War II, when airpower emerged as a powerful military tool. It is essential to guide CSDP properly since "cyberspace reaches its full potential as a warfare domain equal to the traditional ones" (Lee, 2013, p. 59). Valuable lessons from the early years of the aerial domain can be applied to the cyberspace because, without any doubts, as we become involved in a new operating environment, we will find many of the same intellectual puzzles (Hurley, 2012). Nonetheless, we must avoid just expressing existing doctrine in a different way by using the word "cyber" instead of "air" or "space". It can be guessed that now there is a need for resilient and long-lasting cyber defence capabilities so as to support CSDP structures, missions and operations (Council of the EU, 2014).

3. Objectives and research questions

In this paper, the characteristics of cyberspace will be analysed in order to achieve a comprehensive EU approach of cyberspace and collaborate to enhance awareness among the Member States about the need to give cyberspace the scope it deserves as the fifth warfare domain.

Therefore, the objective of this essay is to demonstrate the importance of a Common Security and Defence Strategy in cyberspace. With the help of some real-world examples of cyberattacks, the defining characteristics of the new domain will be examined in order to raise awareness about how cyber-weapons can play a significant role in military operations and the need not only to concentrate EU efforts on the development of capabilities in relation to detection, response and recovery from sophisticated cyber threats (European Commission, 2013) but also on the development of offensive capabilities which will help EU Member States and, consequently, EU as a whole to deter enemy initiatives. Thus, the EU cyber environment will be provided with the necessary security to protect the rights and interests of its citizens and Member States.

Two research questions have been formulated and addressed:

- Which are the defining characteristics which make cyberspace different from the four traditional warfare domains?
- What actions need to be taken within the CSDP framework to give cyberspace the scope it deserves as the fifth warfare domain, thus contributing to make the EU´s cyber environment the safest in the world?

4. Methodology

The elaboration of this paper is based on the detailed analysis of existing documents in the framework of ESS, CSDP and cyberspace. The ESS constitutes the starting point of this research.

4.1. Key documents

The basis to detect possible gaps and begin the analysis of relevant documentation and studies in the field of cyberspace comes from the following documents:

- Cybersecurity Strategy of the EU: An Open, Safe and Secure World formulated by the European Commission (7-2-13) (European Commission, 2013).
- Council of the EU´s conclusions on the Cybersecurity Strategy of the EU: An Open, Safe and Secure World (22-7-13) (Council of the EU, 2013).
- EU Cyber Defence Policy Framework adopted by the Council of the EU (18-11-14) (Council of the EU, 2014).
- European Parliament Report on the implementation of the CSDP (19-3-15) (European Parliament, 2015).

4.2. Complementary documents

The study is complemented with the analysis of important real-world examples of cyberattacks, such as those against the Estonian virtual framework in 2007 or the spread of the worm Stuxnet in 2010 and a varied bibliography of papers and studies of several military authorities and experts in relation to the topic of this paper.

5. Results Discussion

5.1. Defining cyberspace

First attempts to refer to cyberspace as an operational domain were based on the physical world as a defining characteristic (Butler, 2013). Nevertheless, cyberspace is not a Newtonian structure with clear physical laws; it has virtual and cognitive aspects which are not present in the first four war-fighting domains (land, sea, air and space). This implies a high degree of complexity which requires a different way of thinking (Cahanin, 2011). Identifying the unique characteristics of warfare in cyberspace will allow theoreticians to determine how cyber warfare differs markedly from the established doctrine and theory.

5.1.1. Stuxnet: even the most advanced security systems are vulnerable to a sophisticated cyber-attack

In November of 2010, the Iranian President Mahmoud Ahmadinejad publically stated that their nuclear centrifuges had had problems as a result of a computer worm (Erdbrink, 2010). This worm known as Stuxnet is one of the most advanced pieces of malware ever discovered. Specifically designed to target Supervisory Control And Data Acquisition (SCADA) systems and Industrial Control Systems (ICS), Stuxnet succeeded in infecting the computers attached to the Programmable Logic Controllers (PLC) that governed the centrifuges at the Iranian nuclear facility in Natanz. This damaged the centrifuges by spinning them up and slowing them down to the appropriate frequencies for the maximum degradation of the enriched Uranium production. SCADA systems are isolated from any network attempting to achieve an extra grade of security. However, Stuxnet showed that even the most advanced security systems are vulnerable to a sophisticated cyber-attack (Shakarian, 2011). Although the full impact of the worm remains unknown, according to the German computer security expert Ralph Langner: “It will take two years for Iran to get back on track” (Katz, 2010, para. 2).

From a military perspective Stuxnet was a huge success; in fact, it was nearly as effective as a military strike. Stuxnet clearly demonstrates that cyber-weapons can play a significant role in operations, according to that, US former Secretary of Defence Leon Panetta stated in 2011 that: “The potential next Pearl Harbor could very well be a cyberattack” (Ryan, 2011, para. 2).

Stuxnet raised the issue of cyber-discussion, which made research into cyber capabilities more necessary. The effect of Stuxnet on cyberspace was similar to that of the early bombings from World War I on airpower (Lee, 2013).

5.1.2. Estonia 2007: it is often too difficult to know exactly the origin of a cyberattack

Attribution of intrusions and attacks is another important challenge for cyber-security. The way the internet is designed facilitates the issue of anonymity, which together with the ability of some attackers to hide the true origin of an attack makes it difficult to identify them (Hurley, 2012). As former US deputy secretary of defence William J. Lynn claimed in 2011: “Attribution in cyber is always going to be difficult. (…) Missiles come with a return address, cyberattacks do not” (Quinn, Muradian & Weisgerber, 2011, para. 4).

A representative example of the attribution problem in cyberspace are Estonian attacks. Basically, the entire virtual framework within Estonia was overwhelmed with trash for a period of three weeks. Estonian communications network, newspapers, emergency response systems, the state’s largest bank and also the offices of the president, prime minister, parliament, and the foreign ministry were all affected by the attacks (Crosston, 2011).

Estonian and global public perception pointed directly to the Russian government. In fact, Estonian former Foreign Minister Urmas Paet accused the Kremlin of direct involvement in the cyberattacks: "The largest part of these attacks is coming from Russia and from official servers of the authorities of Russia."(Bright, 2007).Nonetheless, Russia always sustained that the attacks came from cyber nation¬alists who acted as a result of patriotism and not obeying orders from any agency or official government office (Crosston, 2011). As

Russian ambassador in Brussels, Vladimir Chizhov, stated: "If you are implying [the attacks] came from Russia or the Russian government, it's a serious allegation that has to be substantiated. Cyber-space is everywhere" (Bright, 2007, para. 11).

The truth is that, despite the Estonian conviction of the Kremlin involvement in the attacks, there was never a final piece of evidence to prove it, which showed that it is often too difficult to know exactly the origin of a cyberattack. The difficulty to trace cyber-culpability seriously hinders efforts made to implement defensive measures (Crosston, 2011).

5.1.3. The defensive capabilities are jeopardised inevitably by the dynamism of cyberspace

The changing nature of information technology is one of the most important challenges for the military operators in the cyberspace domain. This requires rapid and constant adjustments to maintain freedom of action (Cahanin, 2011). Throughout history, the private sector has increased at the pace set for the military conflicts. Nonetheless, in several areas of technological innovation it has now started to grow much more quickly than the defence industry and these rapid changes are a great advantage for attackers. In fact, Gen John E. Hyten, Commander of the US Air Force Space Command, said: "But if you think you´re safe in cyber, when you wake up tomorrow, everything is different" (Babcock, 2015, p. 63).

As found in European Commission (2013, p. 11): "cyberdefense capability development should concentrate on detection, response and recovery from sophisticated cyber threats". However, the cyberspace domain is always dynamic and no matter the defensive countermeasures adopted there will always be an answer to them. Then, the defensive capabilities are jeopardised inevitably by the dynamism of cyberspace, which means that just the offensive capabilities are prone to deterring enemy initiatives (Crosston, 2011).

5.2. Way ahead

On the basis of the points mentioned above, there is an urgent need for EU members to develop appropriate defensive and offensive capabilities in cyberspace. Consequently, an EU Cyberdefence Strategy which sets the guidelines to reach these capabilities is required.

In order to do so, there are some capital actions which have to be taken in order for EU to make its cyber-environment the safest in the world. As General Alexander observed in 2011: "If people who seek to harm us in cyberspace learn that doing so is costly and difficult, we believe we will see their patterns of behaviour change" (Alexander, 2011, p. 9).

5.2.1. Establishment of cyberspace as the fifth warfare domain

The ultimate and clear treatment of cyberspace as a new warfare domain is the first step for CSDP to enforce Member States to step up -without any delay- the development of appropriate cyberdefence capabilities with a comprehensive approach (leadership, organisation, doctrine, staff, training, technology, logistics and interoperability, among others). The aim was to achieve a common level of cybersecurity within the EU (European Parliament, 2015).

5.2.2. Recruitment and training of the necessary skilled human capital

In order for cyberspace to reach its full potential as the fifth warfare domain, one of the priorities is growing and retaining sufficient high quality cyber trained people in our armed forces. Due to the changing nature of cyberspace, individual skills and knowledge will atrophy far more rapidly than in the other domains. Therefore, an extensive investment in the cyber training will be needed, as well as a long-term strategy for developing the cyber culture and educating the next generation of cyberspace operators.

5.2.3. Strengthening of cyberdefence cooperation at all levels

Due to the rapidly changing cyber-environment, it may not be possible to maintain an effective EU´s cyber defence capability without cooperation. As a result, in order to achieve a high common level of cybersecurity, a closer cooperation between Member States will be needed. In that sense, it is not easy for Member States to share their weapon systems or technologies in the other four warfare domains, mainly for a physical reason. Nonetheless, the nature of cyberspace offers plenty of possibilities of expertise and information sharing, especially on the detection of vulnerabilities and threats as well as software improvements.

In addition, cooperation with international partners, particularly with NATO (22 EU´s Member States are members of both organisations), has to be strengthened so as to avoid duplication of efforts (European Commission, 2013). National investment in cyber-capabilities has to be useful for the objectives of both organisations.

Finally, establishing cooperation tools between civilian and military actors in the EU, together with a clear definition of roles in cybersecurity issues are priorities for CSDP in order to optimise human and material resources and avoid possible overlapping in terms of competences.

5.2.4. Cultivation of cyber-mindedness

Owing to the exponential nature of the cyberspace domain and the integration of digital technology that the military encourages in all warfare domains, cyber dependency is steadily growing.

There is no doubt that all military operations currently performed by the EU are cyberspace dependent (Babcock, 2015). This dependency creates strong complementary linkages between the four traditional domains and cyber capabilities. Hence, the new domain must be integrated with joint thinking, which involves the need for EU Member States to consciously train and educate its staff in the application of all cyber capabilities in joint operations.

This joint thinking or cyber-mindedness could be defined as a "comprehensive understanding of cyber power and its optimal application throughout the operational environment" (Coates, 2014, para. 23). CSDP has to promote this comprehensive understanding as the first step for a successful application of cyber power across the whole operational spectrum.

6. Conclusions

Member States in the EU are currently vulnerable to an unexpected and catastrophic cyberattack equivalent to Pearl Harbour. In fact, the European Parliament holds the view that at the moment the Union barely owns the resources needed to contribute in a resolute way to the prevention and management of international crises (including cyber crises) and to assert its strategic interests and autonomy (European Parliament, 2015). Moreover, the exponential growth of cyber dependency in every single aspect of EU's citizens' lives as well as in every military operation led to consider that the following major war will entail attacks in cyberspace. Actually, the majority of analysts, government officials and military specialists point out that life in the twenty-first century will comprise cyberattacks (Cahanin, 2011). Consequently, we must understand the threat of cyber war and start, as an issue of extreme urgency, to develop capabilities for both defence and attack in cyberspace.

The national defence budget reductions due to the economic and financial crisis constitute an important obstacle as regards the Union´s responsibilities in security aspects. Nonetheless, we have to concentrate efforts on making the EU's environment the safest in the world. In order to do so, it is necessary to make a sizeable investment in the training of highly skilled human capital as well as on the renovation and purchase of equipment among Member States.

In view of the real-world examples analysed in this paper, there is no doubt that cyber-weapons can play a significant role in military operations. This fact implies the need for CSDP to recognise cyberspace as the fifth warfare domain, setting guidelines for the development of capabilities among the Member States. Moreover, the CSDP has to promote this development by placing an emphasis on the cooperation as the way to achieve and maintain an effective EU´s cyber defence capability.

The dynamism of cyberspace together with the difficulties in the attribution and the vulnerability of even the most advanced security systems to sophisticated cyberattacks give a great advantage to attackers in cyberspace. Thus, the Member States should continue to develop, improve and refine their defensive technologies but we must not make the mistake of thinking that we will be able to stop our enemies' initiatives only by means of defensive deterrence. We also have to concentrate efforts on the development of offensive capabilities because it is simply easier to attack than to defend in the cyber domain and we have to be ready to exercise, if necessary, our right to self-defence.

Cyber Power means to twenty-first century what Air Power meant to the twentieth century. We have to strengthen our cyber capabilities before a Cyber-Pearl Harbour occurs. Operations in and through cyberspace will demand new tactics, techniques and procedures as well as a joint thinking. Developing a strong cyber-mindedness among the Member States will allow the EU to reach its security objectives at the same time as cyberspace fulfils its full potential as the fifth warfare domain.

"Victory smiles upon those who appreciate the changes in the character of conflict, not upon those who wait to adapt themselves after the changes occur" (Douhet, 1927, p. 1).

Appendix: List of Abbreviations

CSDP:	Common Security and Defence Policy
EU:	European Union
ESS:	European Security Strategy
HR:	High Representative
ICS:	Industrial Control Systems
ICT:	Information and Communication Technologies
NATO:	North Atlantic Treaty Organization
SCADA:	Supervisory Control and Data Acquisition
US:	United States

Cómo citar este artículo / How to cite this paper

Alfaro, J.; Arboleda, I. D. J. (2017). Cyberspace and European security. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 2(2), 71-78. (www.cisdejournal.com)

References

Alexander, K. (2011). Building a New Command in Cyberspace. Strategic Studies Quarterly.

Babcock, C. (2015). Preparing for the cyber battleground of the future. Air & Space Power Journal, 29(6), 61-73.

Bright, A. (2007). Estonia accuses Russia of 'cyberattack'. The Christian Science Monitor. (http://www.csmonitor.com/2007/0517/p99s01-duts.html)

Butler, S. (2013). Refocusing cyber warfare thought. Air & Space Power Journal, 27(1), 44-57.

Cahanin, S. (2011). Principles of War for Cyberspace. Air War College of the United States. Research report.

Coates, J. (2014). Airmindedness: An Essential Element of Air Power. The Royal Canadian Air Force Journal, 3(1). (http://www.rcaf-arc.forces.gc.ca/en/cf-aerospace-warfare-centre/elibrary/journal/2015-vol4-iss3-09-airmindedness.page)

Council of the EU (2013). Council conclusionsontheCommission and the HR of the EU forforeign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the EU: An Open Safe and Secure Cyberspace. Brussels.

Council of the EU. (2014). EU Cyber Defence Policy Framework. Brussels.

Crosston, M. (2011).World gone cyber mad. Strategic Studies Quarterly, 5(1), 100-116.

Douhet, G. (1927). The Command of the Air (Trans. Dino Ferrari). Washington, DC: Office of Air Force History.
Erdbrink, T. (2010). Ahmadinejad: Iran's nuclear program hit by sabotage. Washington Post (29-11-10).
(http://www.washingtonpost.com/wpdyn/content/article/ 2010/11/29/AR2010112903468.html)
European Commission (2013). Joint Communication to the European Parlamient, the Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels.
European Council (2013). European Council 19/20 December 2013 Conclusions. Brussels.
European Parliament (2015). Report on the implementation of the CSDP. Brussels.
HR´s Report on the Implementation of the ESS: Providing Security in a Changing World. Brussels. (2008).
Hurley, M. (2012). For and from cyberspace. Air & Space Power Journal, 26(6), 12-33.
Katz, Y. (2010). Stuxnet virus set back Iran's nuclear program by 2 years. Jerusalem Post (15-12-10).
(http://www.jpost.com/Iranian-Thret/News/Stuxnet-virus-set-back-Irans-nuclear-program-by-2-years)
Lee, R. (2013). The interim years of cyberspace. Air & Space Power Journal, 27(1), 58-79.
Machiavelli, N. (16th-century). The Prince.
Quinn, K.; Muradian, V.; Weisgerber, M. (2011). The Pentagon's New Cyber Strategy. Defense News.
(http://www.defensenews.com/apps/pbcs.dll /article?AID=2011108180316)
Ryan, S. (2011). CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor. ABC News.
(http://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905)
Shakarian, P. (2011). Stuxnet: Cyberwar revolution in military affairs. Small Wars Journal. (http://smallwarsjournal.com/jrnl/art/stuxnet-cyberwar-revolution-in-military-affairs)