UNIVERSITÀ
DEGLI STUDI
FIRENZE

RESEARCH ANALYSIS
2017

THE CYBERTERRORIST THREAT AND THE GOVERNANCE OF THE INTERNET OF EVERYTHING

PABLO MAZURIER

Center for Cyber Security and
International Relations Studies

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell’Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and
International Relations Studies

THE CYBERTERRORIST THREAT AND THE GOVERNANCE OF THE INTERNET OF EVERYTHING

Pablo Mazurier

UNIVERSITÀ
DEGLI STUDI
FIRENZE

Research Analysis

2017

RIGUARDO ALL’AUTORE

Pablo Andrés Mazurier is Ph.D. in Politics, Human Rights and Sustainability at the Sant'Anna School of Advanced Studies, Pisa (Italy) with a research project on Internet Governance. He was a researcher at the King's College, University of London (UK) and at the Institut d'Études Européennes of the Université Libre de Bruxelles (Belgium). He obtained a Master’s degree cum laude in European and International Studies at the University of Trento (Italy), with a thesis on Sociology of Legal Regimes at the Global level, and a full degree in Law at Austral University (Argentina).

THE CYBERTERRORIST THREAT AND THE GOVERNANCE OF THE INTERNET OF EVERYTHING

Introduction.

The purpose of this paper is to study the threat of cyberterrorism as a global socio-political phenomenon which affects not only States and individuals but also the entire internet ecosystem, in particular at the dawn of the Internet of Everything.

The structure of this work is divided in two parts. This paper starts by discussing how cyberterrorism, as well as many other realities such as cybersecurity, innovation and cyberspace, is a social construction. The variation on the perception of cyber terrorism implies important consequences for the internal dynamics of cyberspace and for the actors directly concerned with this phenomenon.

The second part is dedicated to the study of the evolution towards the Internet of Everything, which will reconfigure a complex and dynamic new scenario. If global multistakeholder framework of governance is not adequately implemented, Internet of Everything would exponentially increase the vulnerabilities of the whole cyberspace to be exploited by cyberterrorists.

1. Cyberterrorism and the construction of cyber(in)security.

Terrorism and cyberterrorism is always linked to the State, due to the fact that it represents a public threat to public order and sovereignty. Notwithstanding the multiple factors related to cyberterrorism, Governments have also the power to construct and deconstruct the many narratives which are related to that phenomenon, as an instrument of social control and a way to limit its impact on society. In the case of cyberterrorism, it does not only imply the re-edition of the old threat of terrorism with new tools, but also an opportunity for the governments to reposition themselves in a context characterized by uncertainty, anonymity, dynamism, decentralization and fast spread of unpredictable consequences for most the actors interacting within the cyberspace. Even though globalization and new technologies erode the sovereign power of States, the fight against cyber terror often legitimates governmental control and surveillance over the cyberspace and allows public officials to shift the public attention from its own deficiencies to focus on a specific target. By identifying an antagonistic threat, governments can control the narrative, the agenda-setting and policy-making processes, gaining legitimacy to impose extraordinary measures of control, surveillance and cyber attack[1]. Three examples will serve to illustrate this praxis.

At the end of the 20th century, States and media have used metaphors[2] like "Phantom Menace", "Cyber-Scare", "Cyber Doom", "Cyber-Katrinas", "Guerrilla Warfare in cyberspace" and "Digital Pearl Harbor" to inflate the threat and, indirectly, to highlight how crucial its protective role is for society and how well prepared public forces are to prevent such a critical events to occur. Notwithstanding the construction of a innate insecure cyber scenario, cyberterrorist attacks are no more an abstract threat, as it was affirmed in the past[3], while public and private sectors were spending "less on cyber protection than coffee"[4]. Today, worldwide cybersecurity spending has reached a value of 96 billion dollars[5].

The State models the concept of cyberterrorism to adapt it to its own convenience. During the early beginnings of the internet, when the US were behaving as the champion of free world, the marshal of the post-Cold War international system and the promoter of globalization and capitalism, president Clinton's security analysts increased the narrative of fear[6] and focused the attention on cyber terrorists who were opposing its hegemony. The first G.W. Bush presidency decided to turn towards a more traditional state-oriented vision, shifting its narrative to "rogue States" and their capability to launch cyberwarfare attacks to national critical infrastructure of the US. After the 9/11, under the discursive logic of the "war on terrorism", almost any threat against public and private interests in the cyberspace affecting "interstate or foreign commerce or communication of the United States" is

[1] Erikson, J. (2007), p. 61.

[2] Morozov, E. (2009).

[3] "*The destruction of byts and bytes never directly killed anybody or destroyed any buildings*." Erikson, J. (2007), p. 78.

[4] Ozeren, S. et al. (2007), p. 263.

[5] Hopping, C. (2017).

[6] Erikson, J. and Giacomello, G. (2007), p. 67.

considered an act of "cyberterrorism"[7]. Since then, notwithstanding cyberterrorism was never deprioritized as one of the most fear-mongering scenarios, US government indistinctively used the terms cyberterrorism and cyberwar to descrive different cyber threats, adapting its discourse depending on the magnitude and seriousness of every specific situation.

Both Bush and Obama administrations, notwithstanding their core ideological differences, have constructed a common, strongly symbolic narrative based on the simple idea that the international terrorists use cyber piracy as a source for terrorist fundraising, "robbing billions of dollars" from American economy[8]. In this way they managed to put together three national interests: the fight against terrorism, the international protection of American innovative sector and the legitimacy for governmental extraordinary measures of control, surveillance and attacks in the cyberspace.

As shown in these examples, cyberterrorism is a more complex social phenomenon than the combination of terrorism and cyberspace[9]. Depending on the interests of each actor interacting within the cyberspace, the concept of cyberterrorism uses to be shaped, constructed and described in at least four different interpretations: the objective perspective, the subjective viewpoint, the target conception and the matrix approach.

a) From an *objective perspective*, or *action* perspective, the cyberterrorist act is configured by a list of material key factors. In this traditional explanation[10], the action requires the concurrence of three essential elements: 1) the presence of electronic devices, information technologies and/or internet structures and their data, both as a tool to perpetrate attacks or as target; 2) a terrorist motivation -ideological, ethnical or religious-, and 3) the perpetrator has to be a person or a group of persons, not a State nor a governmental agent acting in the name of a State. These three essential elements are followed by many typical actions: to perpetrate attacks or to perform other actions commonly related

[7] Erickson, J. (2007), p. 72.

[8] McCarthy, D. (2015), p. 137.

[9] Denning, D. (2000), p. 1.

[10] The "traditional picture" of a cyberterrorist attack consists in the use of ICTs and/or internet structure used both as a tool and as a target. Gordon, S. and Ford, R. (2003), p. 7.

with terrorism, such as cyber propaganda, recruitment, organization, logistics, etc.

Each of these three essential elements is necessary to configure a cyberterrorist act. If the action lacks the first element, it might be considered a *terrorist act*. In the case there is not terrorist motivation, it could be considered a *cyber attack* or/and *cybercrime*. And if it lacks the third element, it shall be considered *cyberwarfare* or *informational warfare.*[11]

Fig. 1: Structure of the Cyberterrorist act from an objective perspective.

Essential elements	Actions	Application
1. computer and internet technology used as tool or as target 2. Terrorist motivation (ideological, ethnical, religious) 3. Actor: Single person or Group (not States nor its agents)	A) to perpetrate attacks	In real life: intimidation, blackmailing, threatens human lives[12], to cause relevant material damage[13] or public fear and concern[14], challenging or jeopardizing the State security.
		To online networks/systems, communication infrastructures and data[15]
	B) to act in support or promotion of terrorism	Propaganda, fundraising, recruitment, communication, plotting, indoctrination, radicalization, logistics, planning, material dissemination, support infrastructure.

Focused on the description of the action, the *objective approach* is commonly used for legislative and policy-making aims, due to its

[11] When the action is conducted by a nation-state against another nation's computers or networks, it is considered cyberwarfare. Ayala, L. (2016), p. 49.

[12] New Zealand's law imposes that the attack against an infrastructure facility has to be "likely to endanger life". Chen, T.M. et al. (eds.) (2014), p. 20-21.

[13] For many legislation and academics, violence against persons or severe economic damage are essential elements of cyberterrorism. Conway, M."Cyberterrorism: media myth or clear and present danger?" in: Kan, P.R. and Irwin J (eds)(2004), p. 84.

[14] Cyberattacks lack of the symbolic dimension of theatricality, therefore are less desirable than conventional attacks. Chen, T.M. et al. (eds.) (2014), p. 114-5.

[15] For Addicott, "cyberattacks involve activities that can disrupt, corrupt, deny, or destroy information contained in computers or computer networks." In Ozeren, S. et al. (2007), p. 260.

universal applicability, accuracy, impartiality, internal coherence and integrity on the description of what is and what is not cyberterrorism.

b) The *subjective approach* is not focused on the action but on the perpetrator. This perspective is generally preferred by most of the governmental agencies, in particular during the investigations, not only to prevent future attacks but also to dismantle networks of propaganda, indoctrination and the recruitment of lone-wolves[16]. When a potential terrorist or group is identified, most of the times due to a link with a recognized terrorist organization, the authorities implement techniques of cyber surveillance and data mining on specific social and cyber contexts, although the increasing public concern about social stigmatization and the violation of privacy of the innocent citizens involved in the investigations. Every device, place, action, communication or person connected to the target could be considered as a potential risk for national security. Desouza and Hengsen consider that any usage of the internet by a terrorist constitutes cyberterrorism[17]. However, others argue that an actor-neutral definition of cyberterrorism is preferable[18]. A critical argument of this approach emphasizes the need to shift from this actor-centred conventional view to a more discourse-centered perspective, emphasizing "the intersubjective and constructed nature of terrorism knowledge," the "individual motivations and experiences of terrorists, "their mind-sets and world-views, their 'humiliations and desires'"[19].

c) The *target approach* considers cyberterrorism primarily as "*the use of computer network tools to shut down critical infrastructure*"[20]. It defines the typology by linking a specific medium to a specific target, avoiding any discussion about the perpetrator, the action and the motivation. Although this definition is *per se*

[16] "The most likely scenario that we have to guard against right now ends up being more of a lone-wolf operation than a large, well-coordinated terrorist attack." President Obama address Aug. 16, 2011, cit. in Weimann, G. (2015).

[17] Desouza, K.C. and Hensgen, T. (2003), p. 388.

[18] Stohl, in Chen, T.M. et al. (eds.) (2014), p. 90.

[19] Hülsse, R. and Spencer, A. (2008), p. 574.

[20] Lewis, J. A. (2002).

incomplete[21], it works well as a complementary factor of the latter two approaches. By underlying the criticality of the target, this approach allows authorities, on the one hand, to distinguish between cyberterrorists and political hacktivists[22], and, on the other hand, to focus their policies on preventive actions, consisting in the identification and enforcement of critical infrastructure, the early detection of their vulnerabilities and an adequate plan of protection, risk management and deterrence against cyber attacks.

d) The *matrix approach* considers a list of common elements with no unified hierarchy nor structured classification. These elements are: people (or groups), locations (of perpetrators, facilitators and victims), methods/modes of action, tools, targets, affiliations and motivations[23]. Other study offer a different list, including: Origin of attack—entity (identity of attacker), Origin of attack—system (type of IT and systems), Motivation for attack, Target of attack—entity (population, organization, identity), Target of attack—type, Desired outcome and Results and actual outcome[24]. The advantage of this open approach radicates on its fleasibility, a key characteristic needed to compare different agencies' definitions and to determine how functional task could fit within them[25].

From a constructivist perspective, cyberterrorism constitutes a social reality in constant change, constructed on the basis of discourse, symbols, meaningful experience, reflection, identification and social engagement. The analysis of this phenomenon shifts from what cyberterrorism actually *is* to a more complex question about how cyberterrorism *is perceived*, how it is felt and lived, how it is rhetorically demolished or praised, amplified or minimized. Hence, discourses on cyber security in general, and cyberterrorism in particular, become instrumentalized by interested actors, in particular the State.

[21] Cyberterrorism and cyberwarfare have the same target: to damage critical infrastructures and building control systems linked together within the confines of cyberspace. Ayala, L. (2016), p. 49.

[22] Most would likely agree that disrupting the website of a government department or private organisation, even for political motives, is not an act of terrorism as traditionally understood. Chen, T.M. et al. (2014), p. 2.

[23] Gordon, S. and Ford, R. (2003), p. 5.

[24] Ariely, in Chen, T.M. et al. (2014), p. 178.

[25] Gordon, S. and Ford, R. (2003), op. cit., p. 5.

By exploring the structure of cyberspace, the next part of this study will provide a complete picture of how the discourse of cyberterrorism is adapted to the logic and dynamics of the cyberspace framework.

2. Challenges and Risks of the Internet of Everything.

With the exponential growth of mobile devices[26], applications and social networks, our everyday life is online, generating a huge amount of data[27]. The latest technological challenge is to connect the rest of the objects of our life, maximizing the synergy among the four main elements of this new *Internet of Everything* (*IoE*): people, processes, things and data.[28]

This extremely fast[29] global change represents not only a quantitative[30] but also a qualitative revolution that requires a specific kind of global governance, based on the same multistakeholder, decentralized system used to successfully govern the whole Internet technical structure. But States and key actors from the digital sector are not promoting such solution, and the consequences could generate a strong vulnerability to be exploited by cyberterrorists.

[26] In 1984 there were a thousand devices connected, a million in 1992, ten millions in 2002, one billion in 2008, 10 billion in 2011. Mongay Batalla, J. et al. (eds.) (2017), p. 16. Cisco believes there will be 26.3 billion devices connected to the Internet by 2020, reaching 200 billion if the IoT's miniscule chips are taken into account. Rayes, A. and Salam, S. (2017), p. 26.

[27] During the year 2012 was produced as much data as the whole previous 5,000 years of existence. The current digital universe doubles its data every two days. Turner, V. (2013). Every day the world produces 2 exabytes (2 billion gigabytes). Dahir, H. (et al.) (2015), p. 12.

[28] The new internet will connect people in more relevant ways, will convert data into intelligence to make better decisions, will deliver the right information to the right person or machine at the right time, and will connect physical devices and objects to the internet and each other for intelligent decision-making. Rayes, A. and Salam, S. (2017), p. 3.

[29] Rayes indicates that IoE's rate of adoption is five times faster than that of electricity and telephony growth. Rayes, A. and Salam, S. (2017), p. 23.

[30] Based on Metcalfe's law, which states that the value of a telecommunications network is proportional to the square of the number of connected users of the system (n2). In other words, the more devices and persons are connected, the larger the value of the network.

With the improvement of *Big Data*[31], *Cloud*[32] and *Fog Computing*[33], *Analytics 3.0*[34] and *Artificial Intelligence*, the IoE will exponentially increase the connections between unrelated pieces of information. A fundamental feature of IoE is *context-awareness*, generating automated services and environmental conditions to improve the user's quality of experience[35]. In the new age of *cognitive computing*[36] and *hyper history*[37], machines not only execute restrict tasks but also collaborate with humans, drawing inferences from data thanks to a more rational, analytic and even reflexive process. The center of power will be delocalized, if not relegated, from the direct human use and control of things, to just the design of the code that regulates the connection and interaction between things, mostly at the edge thanks to fog computing. This is the reason why the big corporations are highly focused on leading the dimension of innovation in order to write the code that will rule everything[38].

Taking into consideration how these innovations impact and reshape the whole framework of the Internet technical structure, the Internet of Everything presents both technical and socio-political risks which could be exploited by cyberterrorists.

On the one hand, owing to the classical definition of risk as a function between threat, vulnerability and impact, the IoE affects most specifically the latter two elements. The growth in interconnectedness

[31] Big data consists in massive "volumes of data available in varying degrees of complexity, generated at different velocities and varying degrees of ambiguity that cannot be processed using traditional technologies, processing methods, algorithms, or any commercial off-the-shelf solutions." Kale, V. (2017), p. 208.

[32] The most palpable example of virtualization technologies, Cloud Computing is a digital service which consists of on-demand broad network access to a shared pool of measured computing resources. Kale, V. (2017), p. 177-8.

[33] Fog computing is the expansion of the cloud paradigm, "like a cloud but closer to the edge", extending the architecture into the physical world, providing actions close to the edge without having to send all the volumes of data to the cloud. Dahir, H. (et al.) (2015), p. 13.

[34] Instead of collecting structured and unstructured data from various sources and sending it to a centralized location to be correlated and analyzed, Analytics 3.0 analyze the data close to the source, performing complex processes in microseconds without transferring massive amounts of data through the Internet. Rayes, A. and Salam, S. (2017), p. 19.

[35] Mongay Batalla, J. et al. (eds.) (2017), p. 4

[36] Cognitive computing represents the third era of computing, after the tabulating and programmable systems' periods. Zomaya, A.Y. (2017), p. 814..

[37] Floridi, L. (ed.) (2015).

[38] "[I]n an era in which nation-bound laws regarding content no longer neatly comport with the globally dispersed and decentralized architecture of the global Internet, there is increasing recognition that points of infrastructural control can serve as proxies to regain (or gain) control or manipulate the f low of money, information, and the marketplace of ideas in the digital sphere." Musiani, F. et al. (eds.) (2016).

to trillions of connections[39], most of them at the *edge level*[40] of the fog and cloud computing systems, exponentially increases the vulnerability of the overall system to be hit by cyberattacks, in particular the most common technique of distributed denial-of-service (DDoS) attack[41], which is relatively easy to carry out even by unskilled attackers, very difficult to attribute and dangerous enough to immediately capture social media and public attention. A ubiquitous fog of interconnected, geo-localized and smart sensors demands a higher level of control and human supervision, representing the most vulnerable part of the cyber society of the near future. Hence, the level of impact caused by a cyberattack is directly proportional to the delegation of human supervision in the hands of the AI to control the myriad of devices, services and everyday complex situations. If the only solution to secure this transition to smart computing management is to fortify the internet, then only the technical vulnerabilities would be solved, leaving without solution the main threats, the impact and the overall cybersecurity.

But to enhance a more comprehensive solution, the Internet ecosystem has to focus its attention also on the socio-political feature of cybersecurity. Looking at the big picture, it results essential to maintain an adequate balance and trade-off between the three social dimensions of cyberspace. The systemic risks of fragmentation, erosion of collective trust and consensus, unfinished institutionalization and balkanization of the Internet ecosystem could derivate in extraordinary opportunities for cyberterrorists and cybercriminals to boost their influence and power. In addition to this, the three dynamics of leapfrogging stir up structural vulnerabilities for the entire structure.

By projecting the devices and digital platforms of the future, digital innovation will create new vulnerabilities. If the public sector is not implementing policies to test and control the effects of innovation on the society or if the private sector is only focused on the revenues and there are not enough incentives to invest in making their products and services safer and more secure, the whole cyberspace would be a much dangerous ecosystem. And as a consequence of that, there would be

[39] Mongay Batalla, J. et al. (eds.) (2017), p. 4

[40] The connections at the edge level consist in physical devices and controllers (like sensors, machines, intelligent edge nodes of all types), programmed for several specific tasks and connected with the main network

[41] Rayes, A. and Salam, S. (2017), p. 211.

less incentive to collaborate and to reach institutional consensus in the internet dimension.

Cyberterrorists, considered by Suárez Sánchez-Ocaña as *early adopters* of new technologies[42], would benefit from this situation, exploiting high structural and individual vulnerabilities during the earliest phase of digital implementation.

The main challenge for the international community is to keep on fostering a solid security framework for the Internet and preventing the logic of cyberwarfare to contaminate the collaborative and open environment of the Internet. Reinforcing regional and local capacity-building programs, institutionalizing multistakeholder governance and achieving a long-running engagement between public and private sectors are essential steps to adequately tackle those vulnerabilities.

Since 1998, all US national Administrations combined the discourse of support of a free and open internet with the promotion of a public/private partnership to enforce national cybersecurity. But the private sector, although the fact that it owns the 85% of critical national infrastructure[43], is not willing to assume responsibility in the place of the State[44]. At this point, the cyberwar dimension will keep on being a fertile realm for cyber insecurity[45], a situation that paradoxically would indirectly benefit both the innovation industry and the government.

The corporations will be able to build their cyber fortresses, maintaining the people in a secure but completely controlled environment, and, consequently, the governments will be legitimized to intervene in the cyberspace to limit the superpower of the innovation industry.

[42] Suárez Sánchez-Ocaña, A. (2015), p. 136.

[43] Carr, M. (2016), p. 101.

[44] Carr, M. (2016), p. 103.

[45] Governments and other actors are "*choosing to maintain a state of cyber insecurity*", Carr, M. (2016), p. 184.

3. Conclusion.

Cyberterrorism as a dynamic phenomenon is constantly adapting itself to the logics and interactions depending on the highly uncertain scenario of cyberspace, in particular due to the impact of the Internet of Everything.

Cooperation between main cyber actors is crucial to control cyberterrorism, but it will succeed only if all cyber actors understand and find consensual solutions to both the cyberterrorist phenomenon and the vulnerabilities created by the IoE. A prosperous future for our cyber society depends on finding the *medium virtus* in the context of these narratives, by combining, on the one hand, the salvific power of technological development boosting the IoE and, on the other hand, the increasingly destructive power of the cyber attacks.

Bibliography.

- Abbate, J., (1999), *Inventing the Internet*, The MIT Press, Cambridge-London.
- Akhgar, B. and Brewster, B. (eds.) (2016), *Combatting Cybercrime and Cyberterrorism Challenges. Trends and Priorities*, Springer, New York.
- Aspray, W. and Ceruzzi, P.E. (eds.) (2008), *The Internet and American Business*, The MIT Press, Cambridge Massachussetts
- Ayala, L. (2016), *Cybersecurity Lexicon*, Apress, New York.
- Buchanan, B. (2016) *The cybersecurity Dilemma. Hacking, Trust and Fear between Nations*, Oxford University Press, Oxford.
- Bull, H. (1977), *The Anarchical Society. A Study of Order in World Politics*, Columbia University Press, New York.
- Carr, M. (2016), *US Power and the Internet in International Relations. The Irony of the Information Age*, Palgrave McMillan.
- Ceruzzi, P.E. (2012), *Computing. A Concise History*, MIT Press, Boston.
- Chen, T.M. et al. (eds.) (2014), *Cyberterrorism. Understanding, Assessment, and Response*, Springer, New York.
- Choucri, N. (2012), *Cyberpolitics in International Relations*, The MIT Press, Cambridge-London.
- Dahir, H. (et al.) (2015), *People, Processes, Services, and Things. Using Services Innovation to Enable the Internet of Everything*, Business Expert Press, New York.
- Denning, D. (2000), *"Cyberterrorism. Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services"*, US House of Representatives, 23 May 2000
- Desouza KC, Hensgen T (2003), *Semiotic emergent framework to address the reality of cyberterrorism*, Technol Forecast Soc Change 70(4):388.
- Erikson, J. and Giacomello, G. (2007), *International Relations and Security in the Digital Age*, Routledge, London - New York.
- Floridi, L. (ed.) (2015), *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Springler, New York - London.
- Gordon, S. and Ford, R. (2003), *"Cyberterrorism? Symantec Security Response White Paper"*, Cupertino.
- Hafner, K. and Lyon, M. (1998), *Where Wizards Stay Up Late. The Origins of the Internet*, Touchstone, New York.
- Hertz, N. (2003), *The Silent Takeover. Global Capitalism and the Death of Democracy*, Harper Business, New York.
- Hopping, C. (2017), "*Cyber security spending will hit $96bn in 2018*", in

ITPRO, 12/11/2017, available online: http://www.itpro.co.uk/cyber-security/30122/cybersecurity-spending-will-hit-96bn-in-2018

• Hülsse, R. and Spencer, A. (2008), "*The Metaphor of Terror: Terrorism Studies and the Constructivist Turn*", in Security Dialogue, vol. 39, no. 6

• ICANN's official site, https://www.icann.org/resources/pages/guidelines-2012-05-15-en

• IETF, "*The Tao of IETF*", https://www.ietf.org/tao.html

• Kale, V. (2017) *Big Data computing. A guide for business and technology managers*, CRC Press.

• Kan, P.R. and Irwin J (eds)(2004), *War and virtual war: the challenges to communities*, Rodopi, Amsterdam. 10

• Leiner, B. M. et al. (2003), "*Origins of the Internet*" in "*A Brief History of the Internet version 3.32*", The Internet Society.

• Lewis, J. A. (2002) "*Assessing the Risks of Cyber-terrorism, Cyber War and Other Cyber Threats*", Centre for Strategic and International Studies (Online) http://www.csis.org

• Mayer, M. et al. (2014), "*How Would you define Cyberspace?*", Experimental online Laboratory, Pisa. https://www.academia.edu/7096442/How_would_you_define_Cyberspace

• McCarthy, D. (2015), *Power, Information, Technology, and International Relations Theory. The Power and Politics of US Foreign Policy and Internet*, Palgrave MacMillan, London.

• Mongay Batalla, J. et al. (eds.) (2017), *Beyond the Internet of Things. Everything Interconnected*, Springer, Switzerland.

• Morozov, E. (2009), "*Cyber-Scare:The Exaggerated Fears over Digital Warfare*", Boston Review, July/August 2009. http://bostonreview.net/archives/BR34.4/morozov.php

• Musiani, F. et al. (eds.) (2016), *The Turn to Infrastructure in Internet Governance*, Palgrave MacMillan, New York.

• Nye, J.S. Jr. (2010), "*Cyberpower*", Harvard Kennedy School, May 2010, http://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf

• Nye, J.S.Jr. (2004), *Soft Power: The Means to Success in World Politics*, New York: Public Affairs, x, 5.

• Ohmae, K. (1995), *The End of the Nation State. The Rise of Regional Economies*, Simon and Schuster, New York.

• Ozeren, S. et al. (2007), *Understanding Terrorism: Analysis of Sociological and Psychological Aspects*, IOS Press, Amsterdam.

• Pastor-Satorras, R., Vestignani, A. (2007), *Evolution and Structure of the*

Internet. A Statistical Physics Approach, Cambridge University Press, Cambridge.

• Radu, R. et al. (eds)(2014), *The Evolution of Global Internet Governance. Principles and Policies in the Making*, Springer, New York.
• Rayes, A. and Salam, S. (2017*), Internet of Things - From Hype to Reality. The Road to Digitization*, Springer International Publishing AG, Cham, Switzerland.
• Schia, N.N. (2016), "*Teach a person how to surf": Cyber security as development assistance*, NUPI Report no. 4, Norwegian Institute of International Affairs, Oslo, https://www.files.ethz.ch/isn/196649/NUPI_Report_4_16_Nagelhus_Schia.pdf
• Singer, P. and Friedman, A. (2014), *Cybersecurity and Cyberwar*, Oxford University Press, Oxford.
• Suárez Sánchez-Ocaña, A. (2015), *El quinto elemento*, Ed. Deusto.
• Subrahmanian, V.S. (et al.) (2015), *The Global Cyber-Vulnerability Report*, Springer, Switzerland.
• Telò, M. (ed.) (2007), *European Union and New Regionalism. Regional Actors and Global Governance in a Post-Hegemonic Era*, Ashgate, Hampshire
• Turner, V. (2013) "*The Digital Universe of Opportunities, 7th digital universe study for EMC*", https://www.emc.com/leadership/digital-universe/2014iview/executivesummary.htm
• Weimann, G. (2015), *Terrorism in Cyberspace. The Next Generation*, Columbia Univ. Press, New York.
• Zomaya, A.Y. (2017), *Handbook of Big Data Technologies*, Springer, New York.

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and
International Relations Studies