European Union-Cyber Power in the Making

SLIWISNKI KRZYSZTOF*
Department of Government and International Studies, Hong Kong Baptist University

This article investigates the challenges and limitations of an emerging European cyber security posture. The departure point for the analysis is embedded within the framework that rests on identifying four distinct forms of cyber power: compulsory, institutional, structural and productive.
Tentative conclusions suggest that to be effective, the EU's strategic approach must strike the right balance between all four forms. Additionally, a major challenge for the designers of EU cyber security posture will be accommodating the technology, which due to its characteristics challenges the established balance of power between and within states. Finally, international cooperation regarding two basic categories of cyber threats, whereby states are much more likely to succeed in tackling cyber crime than cyber espionage, must also be addressed.

***Keywords**: European Union, Cyber Security, Cyber Power*

I. INTRODUCTION

Recent years have seen tremendous changes in international relations. As such, 'new world order' is not only devoid of traditional (cold war-type) conflict of ideologies but mainly characterized by economic and socio-political phenomena that are at the bottom of globalization processes. One of the prominent effects of the contemporary ultrafast technological advancement, that drives globalization, is the flourishing of the information technology (IT). Its present-day state of expansion into all spheres of life, including national security, enables us to seriously consider, perhaps first time in human history, the possibility of non-kinetic wars.

It is almost a cliché to say that cyberspace is non-territorial. Its, partly at least, non-physical nature and operation confuses policy-makers and experts alike with regards to strategic options and operational capabilities.

* Department of Government and International Studies, Hong Kong Baptist University, 15 Hong Kong Baptist University Rd., Academic and Administration Bld. F/11, R. 1111, Kowloon Tong, Hong Kong, Tel. 852 3411 5753; E-mail: chris@hkbu.edu.hk

What needs to be kept in mind however is that as Geoffrey Herrera rightly observes, while the nature of cyberspace might not be territorial, its implications for international security are not.[1]

There is a heated debate going on between experts as regards cyber war. Suffice is to say (this paper does not allow a thorough review of the arguments put forward in the discussion) that there is a considering number of the proponents of the idea that we are living in a world that has already experienced examples of cyber wars or acts of aggression, of which probably most would cite Estonia's case of 2007 (to be discussed later in the paper). Others usually present a much more balanced view and claim that IT has been mostly used for espionage, which in itself is seen as nothing special-espionage is arguably part of 'business as usual' in relations between states, be them friendly or not.

Recent cases seem to confirm the letter. When U.S. secretary of State John Kerry and Treasury Secretary Jacob J. Lew visited China for the sixth meeting of the U.S. U.S.-China Strategic and Economic Dialogue (S&ED)[2] in July 2014, one of the major topics they discussed was in deed cyber espionage. Their meeting was undermined by the New York Times report, which indicated an alleged attempt on the part of Chines hackers to break into US federal personnel agency's databases.[3]

At the same time German public opinion and policy-makers were recently shocked to learn that apparently U.S. National Security Agency (NSA) has been spying on highest German officials, including the Chancellor of Germany Angela Merkel.[4] This case in particular is interesting as it shows that two problems in particular. Firstly, even friendly states are willing to go very far in order to obtain information that could be relevant for national security (especially after 9/11). Secondly, inevitably the right to protect private in formation clashes with national security narrative, with the letter one getting an upper-hand.

Amid such challenges, this paper addresses the question of European Union and its potential to act in international relations as a cyber security agent. It builds on the conceptualization of a cyber power presented by

[1] Geoffrey L. Herrera, "Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space" in Myriam Dunn Cavelty, Victor Mauer and Sai Felicia Krishna-Hensel eds, *Power and Security in the Information Age* (Aldershot: Ashgate, 2007), p. 88.

[2] *U.S.-China Strategic and Economic Dialogue to be Held in Beijing, China, on July 9-10, 2014,* U.S. Department of State. *http://www.state.gov/r/pa/prs/ps/2014/06/228571.htm* (accessed 14 July 2014).

[3] "Chinese Hackers Pursue Key Data on U.S. Workers", The New York Times, Asia Pacific, 2014. http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?module=Search&mabReward=relbias%3Aw%2C%7B%222%22%3A%22RI%3A12%22%7D (accessed 14 July 2014).

[4] *Hubert Gude, Jörg Schindler and Fidelius Schmid* "Merkel's Mobile: Germany Launches Investigation into NSA Spying", *Spiegel online International*, *http://www.spiegel.de/international/ germany/germany-expected-to-open-investigation-into-nsa-spying-on-merkel-a-973326.html* (accessed 14 July 2014).

David Betz and Tim Stevens in their seminal book on cyber power: *Cyberspace and the State. Toward a Strategy for Cyber-Power.*

The first part focuses on the conceptualization and institutionalization of cyber security by looking at the cases of USA, UK and NATO. The second part introduces EU as a cyber security agent specifically by referring to its Digital Agenda for Europe. The third and major part addresses the fundamental challenges the EU is facing as an institution in its quest for becoming an effective cyber power.

II. CONCEPTUALIZATION AND INSTITUTIONALIZATION OF CYBER SECURITY

Chinese and American cyber espionage as well as many other cases of hostile cyber acts have prompted experts, academics and decision makers alike to seriously consider cyber space as the fifth domain of warfare.[5] With that realization came the conceptualization of cyber security, threats to cyber security and consequently cyber security strategies (Cyber security has also been considered as an auxiliary or proxy measure, along with trade barriers.[6] Increasingly, countries have been building their economic might more effectively with the help of cyber espionage).

Let us briefly turn our attention to three telling examples of two great powers, namely the US and the UK, and NATO, conceived here as some of the most important stakeholders in the international security realm.[7]

In 2010 after thorough considerations, the US administration set up its Cyber Command (USCYBERCOM) in order to defend American military networks and attack other countries' systems.[8] President Obama identified cybersecurity as one of the most serious economic and national security challenges. Building on the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush, in 2009 the White House carried out a Cyberspace Policy Review that laid foundations for the Executive Branch Cybersecurity Coordinator.[9]

The UK set up their Cyber Security Operations Centre (hosted by Gov-

[5] The other for being traditionally land, air, sea and space see more: Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins, 2010).

[6] "Industry: 'Do not use cyber threat as trade barrier'", EurActiv.com, Home, InfoSociety, News, 2012, http://www.euractiv.com/infosociety/industry-use-cyber-threat-trade-news-513134 (accessed 14 July 2014).

[7] The author's selection is absolutely arbitrary and in that sense reflects only his own approach to the topic at hand.

[8] See more at: http://www.stratcom.mil/factsheets/cyber_command/ (accessed 14 July 2014).

[9] Also referred to as US 'Cyber Czar', Howard Schmidt stepped down in May 2012. See more at: http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator (accessed 14 July 2014).

ernment Communication Headquarters in Cheltenham) and the Office of Cyber Security (set up in the Cabinet Office). In Britain, experts have enhanced the awareness of cyber threats by pointing to vulnerabilities of computer software-run systems present in most spheres of citizens' lives. The latest formulation of the UK's National Security Strategy-'A Strong Britain in an Age of Uncertainty'-reflects this trend by identifying 'Hostile attacks upon UK cyber space by other states and large scale cyber crime' among its priority one risks.[10] It goes on to indicate the roles and responsibilities of individuals, the private sector and the government. It envisages that individual citizens have a great role to play in keeping cyberspace a safe 'place'. In particular, 'everyone, at home and at work, can help identify threats in cyberspace and report them-for example, identifying fraudulent websites.' The bottom line is that just like anywhere in the world, the vast majority of cyber as well as so-called critical infrastructure supervised through computer software is in private hands, that is to say it is not managed directly by governmental bureau-cracies and therefore managed as public goods.

Likewise, NATO has been working to develop adequate capabilities to address cyber threats. In June 2011, NATO defence ministers adopted the Revised Policy on Cyber Defence.[11] Among its highlights is the formulation of a response to cyber attacks. The policy makes clear that if an ally is subjected to some kind of cyber incident, any decision on collective defence (per Article 5 of the NATO Charter that an attack on one is an attack on all) will be a political, not a technical or even military, one.[12] Moreover, a rapid reaction team (RRT) conceived as part of NATO cyber defence capability is on its way to become operational. Its aim will be to offer, upon request, professional and well-organized assistance to its members and partners, especially those countries that do not yet have the resources to set up their own cyber defence capabilities.[13] As a consequence of 2007 Estonia cyber attack NATO also established its Cooperative Cyber Defence Centre of Excellence (CCDCOE)-located in Tallinn. The centre is responsible for conducting technical exercises that allow the participants to learn and test the skills needed to fend off a real attack.[14]

---

[10] *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, Cm 7953, London: The Stationery Office, 2010, p. 27.

[11] See more at: http://www.nato.int/cps/en/natolive/news_75195.htm (accessed 14 July 2014).

[12] Jason Healey, NATO Cyber Defence: Moving Past the Summit, Atlantic Council, 2011, http://www.acus.org/new_atlanticist/nato-cyber-defense-moving-past-summit accessed 20 January 2012 (accessed 14 July 2014).

[13] See more: "NATO Rapid Reaction Team to fight cyber attack", NATO, Homepage, Newsroom, News, 2012. http://www.nato.int/cps/en/SID-81D91D88-E27F9195/natolive/news_85161.htm (accessed 14 July 2014).

[14] See more: NATO Cooperative Cyber Defence Centre for Excellence Tallinn, Estonia, Cyber Defence Exercises, http://www.ccdcoe.org/353.html (accessed 14 July 2014).

1. EU and its Digital Agenda for Europe

In case of the European Union, there is a growing awareness of the need for institutionalizing the response to cyber security threats. The European Network and information Security Agency (ENISA),[15] created in 2004, is located in Heraklion, Crete. As of mid-2014 its objectives are rather moderate and reactive: to make ENISA's website the European 'hub' for exchange of information, best practices and knowledge in the field of information security. Their website is an access point for EU Member States and other stakeholders. One of the most advanced actions to date was the co-organization of 'Cyber Europe 2014' exercise in April 2014,[16] a pan European cyber attack simulation exercise designed to counter simulated attempts by hackers to paralyse critical online services in several EU Member States. The simulation was based on a scenario where Internet connectivity between European countries would be gradually lost or significantly reduced in all participating countries so that citizens, businesses and public institutions would find it difficult to access essential online services. In the exercise, member states needed to cooperate to avoid a simulated total network crash. The exercise proved the importance of communication (procedures and points of contact) between the member states involved and of trust building measures, considering the character of the information to be shared in the event of real attack.[17]

Cyber Europe 2014 is envisaged as part of EU-wide cyber security preparedness exercises under the much broader Digital Agenda for Europe (DAE), one of the seven flagship initiatives under the Europe 2020 strategy that was launched back in March 2010.[18] In this context DAE is supposed to facilitate the delivery of economic and social benefits from a digital single market based on fast and ultra-fast Internet and interoperable

[15] See more: http://www.enisa.europa.eu/about-enisa (accessed 14 July 2014).

[16] See more at: "Biggest EU cyber security exercise to date: Cyber Europe 2014 taking place today", ENISA, available at: http://www.enisa.europa.eu/media/press-releases/biggest-eu-cyber-security-exercise-to-date-cyber-europe-2014-taking-place-today (accessed 14 July 2014).

[17] Previously ENISA organized Cyber Europe 2010. For its self-evaluation report, consult: *Cyber Europe 2010*-Evaluation Report. ENISA-European Network and Information Security Agency, Heraklion: ENISA, 2011, pp. 32-43. Available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2010/ce2010report (accessed 14 July 2014).

[18] See more at *Communication From The Commission To The European Parliament*, The Council, The European Economic And Social Committee And The Committee Of The Regions A Digital Agenda For Europe, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R%2801%29:EN:NOT (accessed 14 July 2014). Europe 2020 Strategy is essentially a plan to 'get Europe back on track' so that it becomes a smart, sustainable and inclusive economy. The EU in this respect has set five ambitious objectives on employment, innovation, education, social inclusion and climate/energy, to be reached by 2020. See more at: http://ec.europa.eu/europe2020/index_en.htm (accessed 14 July 2014).

applications.[19] It specifically identifies problems that are likely to mar the above mentioned objective: fragmentation of digital markets, lack of interoperability, rising cyber crime and risk of low trust in networks, lack of investment in networks, insufficient research and innovation efforts, lack of digital literacy and skills, and finally, missed opportunities in addressing societal challenges.[20] Amid these and other problems there is pressure from the EU Parliament on the Commission to propose harmonised measures to combat cyber crime.[21] Similarly, EU Digital Agenda Commissioner Neelie Kroes recognised the urgent need for an EU-wide strategy against cyber crime.[22] Consequently EU member states have recently agreed to a European Cybercrime Centre to be based at the EU's joint police body, Europol, in The Hague.[23] The next steps included: introduction of the comprehensive strategy for European cyber security, possible agreement among EU institutions on final text of a directive on attacks against information systems and an EU Cybercrime Centre (EC3) ready that was officially commenced on 1 January 2013.[24]

2. Two Kinds of Cyber Threats

In general, cyber threats can be divided into two main categories: illegal activities designed to raise material benefits and national security related actions targeted at states. The first category is associated with transnational organized crime and therefore is mostly affiliated with private actors acting regardless of political agenda. The usual targets are private citizens and businesses; threats in this category are usually referred to as cyber crime or computer crime. Most often the aim of the perpetrators is to acquire information such as private data of customers. The second category, on the other hand, involves political motives such as power maximization, advantage or disadvantage creation etc., and hence involves states or other non-state but politically motivated actors, such as terrorist organizations. Threats under this category involve cyber espionage, cyber terrorism or targeting critical infrastructure.[25]

---

[19] According to EU data The Information and Communication Technologies (ICT) sector is directly responsible for 5% of European GDP, with a market value of €660 billion annually, but it contributes far more to overall productivity growth (20 per cent directly from the ICT sector and 30 per cent from ICT investments) See more: *Ibidem*.

[20] Communication From The Commission, *op. cit*.

[21] "Parliament demands single EU voice on cyber-security", euobserver.com, Focus, 2012, http://euobserver.com/871/116606 (accessed 14 July 2014).

[22] "Kroes demands internet security strategy", euobserver.com, Focus, 2012, http://euobserver.com/871/116019 (accessed 14 July 2014).

[23] "Member states agree to European cyber crime center", euobserver.com, Focus, 2012, http://euobserver.com/1016/116547 (accessed 14 July 2014).

[24] Europol, European Cybercrime Centre (EC3), available at: https://www.eu ropol.europa.eu/content/megamenu/european-cybercrime-centre-ec3-1837 (accessed 14 July 2014).

[25] See more: James A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies, 2002.

Europeans (experts and decision makers) are well aware of cyber crime threats. Politicians and EU bureaucrats, as mentioned before, have been recently calling for the creation of institutional responses. The problems are serious and potentially quite damaging, not only to national economies but also to the EU as a whole. According to Brussels, worldwide more than one million people become victims of cyber crime every day. The cost of cyber crime could reach an overall total of USD388 billion globally.[26] By 2011, nearly three-quarters (73 per cent) of European households had Internet access at home, and in 2010 over one third of EU citizens (36 per cent) were banking online.[27] According to the same source, cyber criminals have created a profitable market around their illegal activities where credit card details can be sold between organized crime groups for as little as €1 per card, a counterfeited physical credit card for around €140 and bank credentials for as little as €60. Recently (as of July 2012) two Security firms, Guardian Analytics and McAfee, published their findings concerning cyber attacks in a joint report called "Dissecting Operation High Roller."[28] According to their findings, Europe has been the primary target for cyber crime related activity such as: Zeus and SpyEye tactics,[29] bypasses for physical multi-factor authentication, automated mule account databases, server-based fraudulent transactions, and attempted transfers to mule business accounts as high as €100,000. In recent years though, the challenges have been spreading to other countries, including the US, whereby cyber attacks have siphoned off at least €60 million from personal and business accounts in 60 banks located in Europe, the US and Latin America.[30] The successful attacks are indiscriminate, that is to say, they target various institutions, well-established and respected major financial institutions as well as small, specialized credit unions and regional banks. Because of the nature of network infrastructure, attacks may include a number of institutions based in various countries at the same time or freely cross national borders, which adds to the complexity of the tasks that national Computer Emergency Response Teams (CERTs) face.

Cyber crime pertains to national security to the degree to which indi-

[26] "An EU Cybercrime Centre to fight online criminals and protect e-consumers, European Commission", Press release, Brussels, 2012, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/317 (accessed 14 July 2014).

[27] *Ibidem.*

[28] Dave Marcus, Ryan Sherstobitoff, *Dissecting Operation High Roller,* White Paper, McAfee An Intel Company (Mission College Boulevard: Santa Clara) http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf (accessed 14 July 2014).

[29] Zeus and SpyEye tactics are simply toolkits that can install malware payloads to control a computer and its applications. The toolkits often deliver web injects to alter browser-based forms and collect password, login and other account information for transmission to an attacker.

[30] "Cyber criminals steal millions from EU banks", euobserver.com, News, 2012, http://euobserver.com/22/116776 (accessed 14 July 2014).

viduals (especially aggregated) and private (financial) institutions are considered to form the backbone of every society. The stability and predictability of everyday economic endeavours add to the certainty of life experience and reflects the broaden conceptualization of security threats including transnational organized crime and the human security perspective.[31] In that context, the latest Eurobarometer survey reveals some interesting and important data. According to the poll, 39 per cent of respondents access the Internet at least several times a day.[32] At the same time, a majority of those questioned (95 per cent) access the Internet from home and work (39 per cent). Around half of all Internet users in the EU say they buy goods or services online (53 per cent), use social networking sites (52 per cent) or do online banking (48 percent), while 20 per cent sell goods or services. Given this, some already alarming numbers have emerged: 12 percent of Internet users across the EU have experienced online fraud, and eight per cent have experienced identity theft. Thirteen per cent have not been able to access online services because of cyber attacks. In addition, more than a third (38 per cent) say they have received a scam email, including ten per cent who say that this is something that has happened to them often. Internet users also express high levels of concern about cyber security: 89 per cent agree that they avoid disclosing personal information online; 74 per cent agree that the risk of becoming a victim of cyber crime has increased in the past year; 72 per cent agree that they are concerned that their online personal information is not kept secure by websites; and finally, 66 per cent agree that they are concerned that information is not kept secure by public authorities.

Traditionally, security has been referred to states. As a referent object, the state has been commonly associated with national security. In this regard, the bureaucratic superstructure of the state, its political system, military capabilities and life-supporting infrastructure form the basis of the cyber security challenge. For its own purpose, ENISA has defined cyber security as referring to the protection of information, information systems, infrastructure and the applications that run on top of it from those threats that are associated with a globally connected environment.[33] As

[31] For an interesting analysis of digital security within human security paradigm refer to: Lene Hansen and Helen Nissenbaum, "Digital Disaster. Cyber Security. and the Copenhagen School". *International Studies Quarterly*. Vol.53. No.3. 2009, pp. 1155-1175. For broader analysis of cyber security and IR theories consult: Johan Eriksson And Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR) relevant Theory?", *International Political Science Review*, Vol.27, No.3, 2006, pp. 221-244.

[32] *Special Eurobarometer 390*, *Cyber Security Report,* (European Commission, July 2012), p. 5. http://ec.europa.eu/public_opinion/archives/ebs/ebs390en.pdf (accessed 14 July 2014).

[33] Udo Helmbrecht, Steve Purser, Maj Ritter Klejnstrup *Cyber security: future challenges and opportunities* (Heraklion: ENISA, 2012), p. 13.

the EU is not a single and unified political actor *per se,* threats in this category mostly refer to EU member states.[34] There is however a clear-cut realization of the need for a coherent pan-European response to securing Europe's ICT systems, since the weakest element of the system (in this case, any EU member state) automatically becomes the loophole through which the security of other member states may be considerably easily compromised. In this regard, the EU has gone through extensive preparatory work that includes evaluation of national cyber security strategies. As of July 2014, only fifteen EU member states have more or less defined national cyber security strategies.[35] To make matters worse, as is usually the case when there is a multiplicity of states, there are different approaches to cyber security as well as threats and challenges among EU members. In spite of certain common themes, there is a fundamental lack of a harmonised definition of Cyber Security at the international level. Consequently the lack of common understandings and approaches between countries may hamper international cooperation, for which all countries acknowledge the need.[36]

3. EU-Cyber Power in the Making

In their insightful analysis of cyber power, David Betz and Tim Stevens emphasize that cyberspace is populated with numerous actors, and it is the actors that make and shape this unique environment: 'From individual citizens to civil society organizations and commercial enterprises, from terrorists and insurgents to branches of state power (militaries, intelligence agencies, etc.) to multilateral global institutions and media conglomerates, from individual nodes to whole networks, and non-humans in the form of hardware and software too.'[37] What connects all of them is global cyberspace, where each and every one has their own ends and strategies. Importantly, this mainly non-physical environment affects power understood as

[34] The Treaty of Lisbon does introduce a legal entity for the European Union, yet from a sheer defence perspective, the EU is still only a grouping of sovereign states that cooperate and coordinate their actions to an extent they deem appropriate. Yet with regards to cyber espionage, EU institutions have been targeted by other states. For example, back in March 2011, when the EU was preparing for one of its summits (this time mainly devoted to the military campaign in Libya, the Euro debt crisis and nuclear safety) the European Commission and External Action Service were hacked into. See more at 'Serious' cyber attack on EU bodies before summit', BBC, News Europe, 2011, http://www.bbc.co.uk/news/world-europe-12840941 (accessed 14 July 2014).

[35] That is as of 30 May 2014 according to: ENISA, National Cyber Security Strategies in the World available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (accessed 14 July 2014).

[36] *Ibidem,* pp. 9-10.

[37] David Betz and Tim Stevens, *Cyberspace and the State. Toward a Strategy for Cyber-Power* (Oxon: Routledge, 2011), p. 38.

a relationship between actors. Essentially, cyber power is not understood as yet another kind or form of power but as a manifestation of the same holistic power in cyberspace. As such, cyber power does manifest itself in four distinct forms: compulsory, institutional, structural and productive.

(1) EU as Compulsory Cyber Power

The compulsory form of cyber power is the most pertinent to the traditional-realist understanding of national power. Whether by direct or indirect coercion, it focuses on modifying the behaviour and conditions of existence of one actor by another. It is understood as compulsory, as much as it is about compelling others to do what we want them to do and what they wouldn't otherwise do.

One has to admit that for obvious reasons the EU does not carry much weight in this category. That is not to say that it has to stay invisible or meaningless. As a form of economic cooperation, the EU has already played an important role in coordinating national policies, which also refers to some extent to foreign security, as well as defence policies of its members. Since actors involved under a coercion paradigm no longer include states only, there is a lot of space for a number of other non-state actors like activists, hackers, criminals, terrorists, states, state proxies, military alliances, private firms, public companies etc. The EU fits perfectly in the picture as far as actions initiated on its behalf. EU bodies, that is, Commissions or particular EU members acting on their own or collectively but each time as members of the same European structure, do intend to modify the behaviour and conditions of existence of other actors in the cyber realm. Just as imposing economic sanctions on Iranian or Korean entities or individuals, the EU may and should be able to operate in the realm of the cyber domain by fighting back to protect data security in the case of cyber crime or cyber espionage, especially if such an attack is directed at EU institutions. In this respect, the already established Computer Emergency Response Team for European Institutions should become a key defensive-offensive tool in future EU cyber security strategy. It is composed of IT security experts from participating EU institutions, including European Commission and others from the European Parliament, the Council, the Committee of the Regions and Economic and Social Committee and ENISA.[38] The team operates under the strategic oversight of an inter-institutional Steering Board. More important than the composition of the team are its designated role and operation procedures.

[38] See more at: http://cert.europa.eu/cert/plainedition/en/cert_about.html (accessed 14 July 2014).

In March-April 2011, European Commission IT experts detected an intrusion in their systems, an attack against the European Union's Emissions Trading Scheme that saw at least €30 million of emissions allowances stolen from national registries.[39] This example not only shows the seriousness of the threat but also calls for the real cyber capabilities of the EU CERT to be established. It calls for the introduction of procedures allowing CERT staff to quickly, preferably with assistance from national CERTs, respond to any kinds of cyber attacks by identifying the threat and deploying offensive tools. That would in consequence mean developing a pan-European cyber defence arsenal.

This might in fact serve as propellant to deepen European integration in the defence field, an idea conceivable and worth pondering, given the fact that the realm of cyber space is supranational by definition. In a non-physical world of electrical impulses, there are no national borders. One might imagine that pooling resources in such an environment would not automatically invoke national sentiments on the parts of governments.[40] Recently governments of some EU members have been acting in a similar fashion. As an example, in 2011, Finland joined Sweden in plans to build an offensive capability as part of its national online defence, all in order to create malware and exploits to launch online counter-attacks to threats. As Defence Permanent Secretary Lt Gen. Arto Räty asserted: 'Attack is an unfortunate word, but there can be no defensive capability without the ability to offer a counter-punch. The two things go hand in hand.'[41]

(2) EU as Institutional Cyber Power

Institutional cyber power rests on indirect control of one actor's 'manoeuvring field' through third party formal and informal institutions. In this respect, the most powerful actors are able to set norms and standards that ultimately shape the environment in which they themselves and all other actors exist and through which they try to arrive at their goals.[42]

This part of the paper will address two elementary avenues for an institution such as the EU to shape its institutional component of cyber power:

---

[39] *Ibidem.*

[40] This coincides with the paradigm of 'epistemic communities' and the role of knowledge in rational strategic calculations. For an introductory analysis of the role of epistemic communities in international relations refer to Emanuel Adler, "The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the Idea of Nuclear Arms Control", *International Organization*, Vol.46, No.1, 1992, pp. 101-145. Or Emanuel Adler and Peter M. Haas, "Conclusion: Epistemic Communities, World Order, and the Creation of a Reflective Research Program", *International Organization*, Vol.46, No.1, 1992, pp. 367-390.

[41] "Scandinavia wants cyberwar weapons", Secure Business Intelligence, 2011, http://www.scmagazine.com.au/Tools/Print.aspx?CIID=277767 (accessed 14 July 2014).

[42] David Betz and Tim Stevens, *Cyberspace and the State ⋯ op. cit.*, p. 47.

international cooperation and facilitation of member states' approaches to cyber security threats.

- **International Cooperation**

When dealing with global security threats and challenges, such as those referring to the cyber domain, it is almost a cliché to notice that the response on the part of national governments needs to cut across traditional lines of dividing organizational structures. In that respect there has been a realization within the EU Parliament, The Commission and ENISA especially that without international cooperation, including a high level of institutionalization and socialization alike, an effective EU response to cyber security threats has limited prospects. Cooperation, therefore, should not only include EU member states but other major stakeholders like China or the US. Such cooperation will definitely be easier when it comes to first of the earlier mentioned threats, cyber crime, rather than the second, cyber espionage or cyber attacks, since most states tend to treat the later as proxy to economic competition.

As regards US and EU cooperation, it has been developed under the general framework of the trans-Atlantic cooperation in cyber security that allows the creation of the concurrence. In particular the EU-US Working Group on Cyber-security and Cyber-Crime has been established.[43] For the time being, focus is put on organizing events like the one on 12 June, 2012, devoted to gathering all potential intermediaries together to exchange experiences both from the EU and US sides.[44] Alliance between these two is vital, as both pretend to be major shareholders in international (cyber) security (generating a huge volume of electronic trade or running critical infrastructure that is highly dependent on computer systems). Awareness raising exercises as well as sharing the pool of experience are undoubtedly important, but fundamental problems seem to limit the effectiveness. First, there seems to be a lack of clarity as regards the institutional side of the matter. As already mentioned in this paper, the NATO rapid reaction team (RRT) seems to focus more on the American side of the Atlantic. The US has signed and ratified the Council of Europe Convention on Cyber Crime (which conveys a common commitment to punish perpetrators and to deter cyber threats), but some of the EU members like Poland or Greece have not.[45] Also, there is an essential problem

[43] See more at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/246 (accessed 14 July 2014).
[44] See more at: http://www.enisa.europa.eu/activities/cert/security-month/eu-us-event-on-intermediaries-in-cyber-security-awareness-raising (accessed 14 July 2014).
[45] As of 14 July 2014, see more at: Convention on Cybercrime CETS No.185, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (accessed 14 July 2014).

with the lack of a commonly agreed definition of cyber defence among EU members as well as between the EU and US. Finally, there is the question of the International Treaty on Cyberwar. As much as the idea is supported in some EU member states, it is generally frowned upon by the American administration. As Richard Clarke rightly indicated, depending on the agreed definition of cyber warfare, a global cyber treaty might in effect only limit the US in carrying out some of the activities like cyber espionage, 'but it is extremely doubtful that some other nations would.'[46] Worse still, such a document would have to be channelled through the UN, which is notorious for its slow responsiveness to pressing threats to various levels of security. International law itself is outdated, on top of which there is no clear vision among members of the international community as to how it should encapsulate cyber war.[47] The UN Charter for that matter was drafted during the time when the Internet was unimaginable and the most advanced equipment in the realm of computation and information were probably Enigma, used by Germans during the Second World War, and huge programmable computing machines that would take up the space of whole rooms.[48]

As for other major stakeholders, the EU has recently been pursuing the issue of cyber security in its talks with Chinese officials. The Joint Press Communiqué of the recent 14th EU-China summit of 14 Feb 2012 recognizes the importance of 'deepening understanding and trust on cyber issues.'[49] What this means in practice is that EU and China will set up an EU-China Cyber Taskforce. As of now, the aims of the taskforce seem moderate to say the least: address common cyber threats through enhanced bilateral exchanges and cooperation. It is also supposed to promote and develop technologies related to information and communication security, with a view to fostering economic and social development.[50] The basic problem is that China and the EU have different concepts of cyber security or the cyber realm in general. Its strategic partnership set up back in 2003 remains highly declaratory and trade focused.[51] China has also

[46] Richard A. Clarke and Robert Knake, *Cyber War … op. cit.*, p. 235.

[47] Nat Katin-Borland, "Cyberwar: A Real and Growing Threat", *Cyberspaces and Global Affairs*, eds Sean S. Costigan and Jake Perry, Farnham: Ashgate, 2012, p. 17.

[48] See more at Edmund Callis Berkeley, *Giant Brains; or, Machines that Think*, New York: Wiley, 1949.

[49] Joint Press Communiqué of the 14th EU-China Summit, Council of The European Union, http://eeas.europa.eu/china/summit/summit_docs/ 120214_joint_statement_14 th _eu_china_summit_en.pdf (accessed 14 July 2014).

[50] Zhongqi Pan, 'After the China-EU summit: reaffirming a comprehensive strategic partnership', *European Strategic Partnership Observatory, Policy Brief*, Vol.3, 2012, p. 3.

[51] See more at David Scott, "China and the EU: A Strategic Axis for the Twenty-First Century?", *International Relations*, Vol.21, No.1, 2007, pp. 23-45, Also: Jonathan Holslag, "The elusive axis Evaluating the EU-China strategic partnership", *The Asia Papers*, *Brussels Institute of Contemporary China Studies*, Vol.3, No.8, 2009, pp. 1-33.

been identified as being behind some serious acts of cyber espionage against states as well as private enterprises. According to the *Financial Times,* Chinese authorities have been for some time developing cyber militias affiliated with the People's Liberation Army. An example quoted by the *FT* includes a midsized tech company employing around 500 employees. Supposedly all staff under the age of 30 belong to a special unit within the given company that allegedly focuses on cyber attack and cyber defence.[52] These, along with hundreds of thousands of young people from other tech companies and universities all over the country, form the backbone of Chinese cyber warriors.

As for Russia, the situation is somewhat similar. Matters revolving around cyber security (mainly cyber crime) are covered by the Partnership and Cooperation Agreement and more specifically by one of its four common spaces, namely: Common Space of Freedom, Security and Justice.[53] Yet, in recent years the cooperation between the EU and Russia has not been flourishing, mainly due to human rights disputes, visa requirements for Russian citizens willing to travel to EU countries, difficulties for Russians living in Kaliningrad to reach other parts of Russia, energy (as Russia has a significant role in the European energy sector), and security issues including Poland, the Czech Republic or Romania and cooperation with the US and consequent involvement in US ballistic missile defence. In the meantime Russia has been heavily criticised by Europeans for its involvement in the crisis in Georgia in 2008 as well as its 'unreliable' stance when it comes to Libya in 2011, and most importantly Syria in 2012. With Putin back as President of the Russian Federation, many observers expect the continuation of tensions and limited progress.[54] As for cyber security issues, Russia is still perceived in Europe with great unease given its attack on Estonia in 2007, as some term it the first instance of cyber warfare, an effect over which NATO countries established a NATO Cyber Defence Centre in Tallinn.[55]

---

[52] "Chinese military mobilizes cyber militias", Ft.com, World, Asia Pacific, China, 2011, http://www.ft.com/cms/s/0/33dc83e4-c800-11e0-9501-00144feabdc0.html#axzz1bloadgXj (accessed 14 July 2014).

[53] See more at: http://eur-lex.europa.eu/LexUriServ/LexUriServ. do?uri=CELEX:21997A1128(01): EN: NOT (accessed 14 July 2014).

[54] Latest EU-Russia summit in St Petersburg, 2012, was a well-prepared and carried out diplomatic show designed to steer clear of most of the controversial issues and emphasize harmony between both sides. For example: "EU-RUSSIA SUMMIT (St Petersburg, 3/4 June 2012)", Europa, Press Releases RAPID, Brussels, 2012, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/401&type=HTML (accessed 14 July 2014).

[55] An attack that apart from targeting essential electronic infrastructure of the state and therefore affecting most of the Estonian population also caused huge economic losses. For example, Estonia's Hansbank reported losses over US$1 million. See more at Mite Valentinas, "Estonia: Attacks Seen As First Case Of 'Cyberwar'", *Radio Free Europe*, *Radio Liberty*, 2007. http://www.rferl.org/content/article/1076805.html (accessed 14 July 2014).

- **Public-Private Partnership?**

The EU's prime institution responsible for exchange of information, best practices and knowledge in the field of information security, ENISA, has been assisting EU member states in the task of developing and maintaining their own national cyber security strategies. For this purpose, ENISA has prepared a 'Good Practice Guide',[56] designed as a study on national cyber security strategies in order to highlight good practices and recommendations on how to develop, implement and maintain a cyber security strategy. As such, the Good Practice Guide is meant to be a useful tool and practical advice for those responsible for and involved in cyber security strategies. It involves experts from the public sector and stakeholders from the private sector across Europe who finalized their work by the end of 2012.

At the same time, The European Commission is trying to push energy, transport and financial companies operating in the EU to invest more in their cyber security and to report on any breaches that could compromise their security. Pertinent to the role and significance of 'critical infrastructure', private entities are part of the same system, and the system itself is as weak as its weakest element. Therefore the Commission plans to extend security breach notifications to new industries other than telecommunication companies and Internet firms, which in Europe are already subject to reporting obligations.[57]

On top of that, the EU legal system already stipulates that illegally accessing and interfering with computers, servers and data is punishable by criminal law.[58] It also specifically aims to address and punish those who build, use and sell tools and software designed to carry out cyber attacks, including criminal groups that launch malware and botnets against sensitive information infrastructure in EU countries. Along these lines the directive of the European Parliament and of the Council on attacks against information systems' introduces a specific combination of non-legislative measures that focus on cross-border law enforcement and public-private cooperation and the introduction of specific targeted (that is, limited) legislation to prevent large-scale attacks against information systems.[59]

---

[56] See more at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss (accessed 14 July 2014).

[57] Refer to: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Official Journal L 201, 31/07/2002 P. 0037-0047. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML (accessed 14 July 2014).

[58] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *Official Journal L 069, 16/03/2005 pp. 0067-0071*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:HTML (accessed 14 July 2014).

[59] Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, Brussels, COM (2010) 517 2010/0273 (COD), p. 6, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF (accessed 14 July 2014).

(3) EU as Structural Cyber Power

Addressing the long existing methodological conundrum of actors vs. structure, structural cyber-power is best understood as one that allows a particular actor (the most powerful) to uphold the structures of power relations in which all actors are positioned and which in turn permit or constrain their actions.[60] It is closely related to the concept of 'information society', which rests on collecting and manipulating data, information and knowledge.[61]

The cyber domain does offer new possibilities to some previously 'underprivileged' actors. The Internet is a global electronic empowering tool through which a plethora of resistance activities takes place, changing the traditionally established balance of power within political systems. Recent examples from North Africa and the Middle East attest to the role of cyber space in creating networks of concerned citizens displaying their outrage at local governments.[62]

This is also pertinent to the idea of 'civilianization' of security, a notion relating to non-military, voluntary organisations and the business/private sector, engaged by government but acting in their own right, to prevent, protect and prepare in the context of a counterterrorism strategy. With regards to cyber security, it is a phenomenon by which ordinary civilians act as providers of their own security. Since governments and public institutions have become increasingly inefficient in providing security to citizens, especially when one takes an individual as security 'referent', it remains for private entities and non-public bodies to fill the vacuum.[63] In fact, EU documents increasingly emphasize the potential for individuals and public/private partnership especially in the fight against cyber crime. EUROPOL for that matter is planning to get net users directly involved in catching cyber crime gangs.[64] This would supposedly empower EU

---

[60] David Betz and Tim Stevens, *Cyberspace and the State … op. cit.*, p. 49.

[61] An interesting and insightful analysis of knowledge-based economy is provided by Alvin and Heidi Toffler in one of their latest books, *Revolutionary Wealth* (New York: Alfred A Knopf, 2006), p. 100.

[62] Much has recently been written and published on the role of Internet-based social media in China, whereby citizens are able to by-pass state control of the distribution of information and effectively influence local governments. See more at: Using ICTs to create a culture of transparency: John C. Bertot, Paul T. Jaeger, Justin M. Grimes, "E-government and social media as openness and anti-corruption tools for societies", *Government Information Quarterly*, Vol.27, No.3, 2010, pp. 264-271, Or: Haiqing Yu, "Blogging Everyday Life in Chinese Internet Culture", *Asian Studies Review*, Vol.31, No.4, 2007, pp. 423-433. Also: Rebecca MacKinnon, "China's 'Networked Authoritarianism'", *Journal of Democracy*, Vol.22, No.2, 2011, pp. 32-46.

[63] Krzysztof Śliwiński, "Counter-terrorism-a comprehensive approach. Social mobilization and 'civilianization' of security: the Case of the United Kingdom", *European Security*, 20 12, pp. 1-19, iFirst article, DOI: 10.1080/09662839.2011.584308.

[64] Brian Wheeler, "EU could turn to 'crowd sourcing' in cyber crime fight", BBC News, UK Politics, 2010. http://www.bbc.co.uk/news/uk-politics-12004134 (accessed 14 July 2014).

citizens not only to look out for themselves but also to report criminal activity. This 'crowd-sourcing plan', though in its embryonic stages, will depend on the functioning of the European Cybercrime Centre (mentioned earlier in this paper) that has recently started operating within the framework of EUROPOL.

(4) EU as productive cyber power

Finally, and perhaps most importantly, productive forms of cyber-power underpin all the above mentioned. As a partly non-physical environment, cyberspace 'serves to reproduce and reinforce existing discourses, as well as to construct and disseminate new ones.'[65] The idea is that such constructed social beings enable social relations, through which power may be exercised. This form of cyber-power is manifested by identifying certain actors as threats to national security, which in turn allows states to treat them as legitimate targets.[66]

Practicalities of cyber threats make it increasingly difficult for states or groupings of states to attribute challenges, threats or attacks, should they take place, with any particular agents. The nonphysical, transnational and imminent character of information networks best epitomizes what security experts refer to as an 'attribution problem.' Consequently this testifies to further confusion with regards to legitimate objects for states' supervision.

Let us take a look at the ENISA approach to this issue. In one of its latest publications, *Cyber Security: future challenges and opportunities*, a document that will most likely serve as the basis for future pan-European cyber security strategy, we read: 'In the past, troops from opposing countries confronted each other on a battlefield, and "rules" for warfare were written if not always followed. The Geneva Convention, for example, describes rules for the protection of people who do not take part in the fighting. Outside these rules, terrorist organizations seek to achieve mainly political aims by operations, which, under state legislation, are assessed as criminal acts. With Internet technology it is possible for an individual, group or state to carry out remotely controlled, often covert, cyber attacks on critical infrastructures of a state. Therefore the line between soldier, terrorist and criminal becomes blurred.'

Most of the communication concerning cyber security that flows from Brussels focuses on non-state actors. EU institutions as well as EU bureaucrats of various levels increasingly refer to cyber security through the lens

[65] David Betz and Tim Stevens, *Cyberspace and the State* ··· *op. cit*., p. 51.
[66] It is exemplified by the evolution of the meaning of the term 'hacker' and derived forms such as 'hacktivists' or parallel terms such as 'e-crime/cybercrime', 'cyber terrorist/terrorism.'

of non-state actors. Their narratives are full of references to individuals, transnational organized crime, terrorists or simply criminals, further undermining a realistic conception of national security. Therefore it is the contention of the author of this paper that the productive power of the EU in the field of cyber security seems to be driving the conceptualization of security towards its human aspects (human security) and a social constructivist approach (a tool such as the Internet is neutral so long as it is used against the security of a particular referent object, in which case it acquires negative characteristics and can be understood as a threat).

On the other hand, non-state actors are increasingly challenging both states and supranational structures. States' soft power in that respect is countered by a peculiar soft power of international terrorist organizations or transnational organized crime. Cyberspace in this regard offers tangible opportunities for non-state actors' growth of soft power. The state-centric bureaucratic apparatus proves simply too slow and not flexible enough to meet the challenges of governability in the 21st century.[67] Coupled with the current financial situation, the recent phenomenon of privatization of war[68] as well as privatization of security, the EU is more than likely to stumble in its quest to effectively address its cyber security.

III. CONCLUSION-MEETING THE CHALLENGES AHEAD

In October 1932, Harold J. Laski wrote in his paper about the inability of Europe to efficiently respond to threats of communism and fascism. His words are still more than relevant with regards to limitations and weaknesses of the EU.

> *… the myth of national sovereignty, the failure to respect the League, all of these were implicit in its ultimate disrespect for moral principle. The social habits of its votaries, its literature with its insistent note of cynical skepticism,*

[67] For an interesting analysis of the crisis of governability in advanced industrial democracies and its consequences to future stability of democratic regimes refer to: Charles A. Cupchan, "The Democratic Malaise" in Gideon Rose and Jonathan Tepperman eds, *The Clash of Ideas. The Ideological Battles that Made the Modern World a And Will Shape the Future* (New York: Foreign Affairs, 2012), Kindle Version, loc., pp. 5439-5587.

[68] Writing at the very beginning of the 1990s, Van Creveld seems to have made the right point about future wars that are decreasingly fought by regular armies and increasingly by terrorists, guerrillas, bandits and robbers. Urban crime may, as he asserted, "develop into low-intensity conflict by coalescing along racial, religious, social, and political lines". As small-scale violence multiplies at home and abroad, state armies will continue to shrink, being gradually replaced by a booming private security business, as in West Africa, and by urban mafias, especially in the former communist world, who may be better equipped than municipal police forces to grant physical protection to local inhabitants. See more at: Martin Van Creveld, *Transformation of War*, New York: The Free Press, 1991, p. 41.

its philosophy which sought refuge in mysticism and impulse to shut out the still small voice of reason, a press which (not least notably in its dealing with Russia) could make miraculous propaganda but could not tell the truth, its religions in decay, its political and economic institutions hopelessly remote from the realities they confronted, its leaders like straws caught in the eddies of an ever-quickening stream-it is not in such a society as this that one looks for the spring of a new hope.(…) Such a society cannot meet the challenge of communism, because its faith in itself is not sufficient to give it a victorious destiny. It may postpone defeat; it cannot finally elude it. For in the conflict of the future looks bleak unless liberalism can reform itself.[69]

EU recently issued its first cyber security strategy in a document titled 'EU Cyber Security Strategy-open, safe and secure.'[70] Though impressive at first sight, through reading reveals serious questions regarding the potential for EU to effectively influence its environment as a cyber security agent. Four issues seem of utmost importance. First, international cooperation, especially when referring to cyber espionage, is less than likely to come to fruition in the nearest future for simple but prevailing reasons of divergent interests and the consequent competition between states. In that sense, coordination of national strategies for cyber security of EU member states is the most the EU as an actor can aim at. Additionally, strong cooperation with key partners such as the US or Israel is feasible.

Second, technology does change the balance of power between and within states. In that respect the Internet, just like the printing press before it, provides the masses with easy access to information, creating large pools of pressure on those who govern. Security strategies need to accommodate these challenges. Practice shows that technological developments in general and communication liberalization empowers individuals or private entities, which can provide states with an 'extra hand' in their fight against cyber crime or the protection of critical infrastructure.

Third, the future EU cyber security posture should incorporate, if not verbally, then in principle, four different forms of cyber power: compulsory, institutional, structural and productive. Only a balanced combination of all four forms will allow a truly strategic approach, and without which Harold Laski's words might again prove prophetic. Europeans need to understand that the 'creeping threats' to cyber security continue to affect not only the security of their states but also their individual human

[69] Harold J. Laski, "Position and Prospects of Communism", in Gideon Rose and Jonathan Tepperman (eds), *The Clash of Ideas. The Ideological Battles that Made the Modern World - And will Shape the Future*, New York: Foreign Affairs, 2012, Kindle edition, location, pp. 3094-3108.

[70] EU Cyber Security Strategy-open, safe and secure. Available at: http://eeas.europa.eu/top_stories/2013/070213_cybersecurity_en.htm (accessed 14 July 2014).

safety, which in turn requires some sort of compromise between freedoms and security.[71]

Finally, in the future EU needs to clarify what is actually meant when the terms 'cyber security' or 'cyber security strategy' are in use. Contemporary understandings offered by ENISA lack clear focus and seem to be sweeping and general, which obviously constitutes a challenge to any operational capabilities that will no doubt be developed in the future. EU cyber security strategy needs to achieve much more than merely coordinating national actions. What is needed in fact is supra-natural understanding of challenges and threats and the tools that are feasible to address them. It is the contention of the author of this paper that such an approach will further 'Europeanize' particular states' security policies, perhaps with the help of well researched mechanisms of 'spill over' that have characterized the process of European Integration for so long.[72]

REFERENCES

A Strong Britain in an Age of Uncertainty: The National Security Strategy, Cm 7953 (London: The Stationery Office, October 2010), p. 27.

Alvin and Heidi Toffler, *Revolutionary Wealth*, New York: Alfred A Knopf, 2006.

Charles A. Cupchan, "The Democratic Malaise' in Gideon Rose and Jonathan Tepperman eds", *The Clash of Ideas. The Ideological Battles that Made the Modern World a And Will Shape the Future*, New York: Foreign Affairs, 2012.

Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions A Digital Agenda For Europe, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R%2801%29:EN:NOT

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *Official Journal L 069, 16/03/2005 p. 0067-0071*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:HTML.

Cyber Europe 2010-Evaluation Report. ENISA-European Network and

[71] In the seemingly inescapable conundrum of freedom vs. security, at least some of its aspects might be effectively addressed by the 'privatization of security', which is what has been pursued for some time in the case of the UK.

[72] For the time being, the EU commission does realize and has acknowledged on numerous occasions the fact that many among EU member states are ill-equipped and in consequence totally unprepared for future cyber threats. See more at: Nikolaj Nielsen, "EU cyber-security legislation on the horizon", euobserver.com, News, Justice and Home Affairs, 2012, http://euobserver.com/22/116239 (accessed 14 July 2014).

Information Security Agency, Heraklion: ENISA, 2011, pp. 32-43. Available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2010/ce2010report.

Dave Marcus, Ryan Sherstobitoff, *Dissecting Operation High Roller,* White Paper, McAfee An Intel Company (Mission College Boulevard: Santa Clara) http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf.

David Betz and Tim Stevens, *Cyberspace and the State. Toward a Strategy for Cyber-Power*, Oxon: Routledge, 2011.

David Scott, 'China and the EU: A Strategic Axis for the Twenty-First Century?', *International Relations*, Vol.21, No.1, 2007, pp. 23-45.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Official Journal L 201, 31/07/2002 pp. 0037-0047, http://eur-lex.europa.eu/LexUriServ Serv/LexUri Serv.do?uri=CELEX:32002L0058:EN:HTML.

Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, Brussels, COM (2010) 517 2010/ 0273 (COD), p. 6. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF.

Edmund Callis Berkeley, *Giant Brains; or, Machines that Think*, New York: Wiley, 1949.

Emanuel Adler and Peter M. Haas, 'Conclusion: Epistemic Communities, World Order, and the Creation of a Reflective Research Program', *International Organization*, Vol.46, No.1, 1992, pp. 367-390.

Emanuel Adler, "The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the Idea of Nuclear Arms Control", *International Organization*, Vol.46, No.1, 1992, pp. 101-145.

EU Cyber Security Strategy-open, safe and secure. Available at: http:// eeas.europa.eu/top stories/2013/070213 cybersecurity en.htm.

For broader analysis of cyber security and IR theories consult: Johan Eriksson And Giampiero Giacomello, 'The Information Revolution, Security, and International Relations: (IR) relevant Theory?', *International Political Science Review*, Vol.27, No.3, 2006, pp. 221-244.

Geoffrey L. Herrera, "Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space", in Myriam Dunn Cavelty, Victor Mauer and Sai Felicia Krishna-Hensel eds, *Power and Security in the Information Age*, Aldershot: Ashgate, 2007.

Haiqing Yu, " Blogging Everyday Life in Chinese Internet Culture", *Asian Studies Review*, Vol.31, No.4, 2007, pp. 423-433.

Harold J. Laski, "Position and Prospects of Communism", in Gideon Rose

and Jonathan Tepperman (eds), *The Clash of Ideas. The Ideological Battles that Made the Modern World-And will Shape the Future*, New York: Foreign Affairs, 2012.

James A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies, 2002.

Jason Healey, NATO Cyber Defence: Moving Past the Summit, Atlantic Council, 2011. http://www.acus.org/new_atlanticist/nato-cyber-defense-moving-past-summit accessed 20 January 2012

John C. Bertot, Paul T. Jaeger, Justin M. Grimes, "E-government and social media as openness and anti-corruption tools for societies", *Government Information Quarterly*, Vol.27, No.3, 2010, pp. 264-271.

Jonathan Holslag, "The elusive axis Evaluating the EU-China strategic partnership", *The Asia Papers, Brussels Institute of Contemporary China Studies*, Vol.3, No.8, 2009, pp. 1-33.

Krzysztof Śliwiński, "Counter-terrorism-a comprehensive approach. Social mobilization and 'civilianization' of security: the Case of the United Kingdom", *European Security*, 2012, pp. 1-19, iFirst article | DOI: 10.1080/09662839.2011.584308.

Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School", *International Studies Quarterly*, Vol.53, No.3, 2009, pp. 1155-1175.

Martin Van Creveld, *Transformation of War*, New York: The Free Press, 1991.

Nat Katin-Borland, "Cyberwar: A Real and Growing Threat", *Cyberspaces and Global Affairs*, eds Sean S. Costigan and Jake Perry, Farnham: Ashgate, 2012.

NATO Cooperative Cyber Defence Centre for Excellence Tallinn, Estonia, Cyber Defence Exercises, http://www.ccdcoe.org/353.html

Rebecca MacKinnon, "China's 'Networked Authoritarianism'", *Journal of Democracy*, Vol.22, No.2, 2011, pp. 32-46.

Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, New York: Harper Collins, 2010.

Special Eurobarometer 390. Cyber Security Report, European Commission, 2012, p. 5. http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf.

Udo Helmbrecht, Steve Purser, Maj Ritter Klejnstrup *Cyber security: future challenges and opportunities*, Heraklion: ENISA, 2012.

Zhongqi Pan, "After the China-EU summit: reaffirming a comprehensive strategic partnership", *European Strategic Partnership Observatory, Policy Brief*, Vol.3, 2012.