Moving beyond the European Union's Weakness as a Cyber-Security Agent

SLIWINSKI, Krzysztof

Published in:
Contemporary Security Policy

DOI:
10.1080/13523260.2014.959261

Published: 02/09/2014

Moving beyond the European Union's Weakness as a Cyber-Security Agent

Abstract: Policy and research on European cyber-security remains formative compared to leaders in the field like China and the United States. This article evaluates the European Union (EU) as a cyber-security actor, asking fundamental questions concerning the EU's combination of prominence and obscurity, especially its limitations and prospects. Who and what is going to dominate the European response to cyber-security in the future? These questions are examined within the larger framework of liberal intergovernmentalism. The EU also is compared to the North Atlantic Treaty Organization (NATO), a point of reference to further understand the limitations and challenges ahead for the EU. Two major factors limit the EU as a cyber-security actor: its intergovernmental character, and the lack of collective vision on cyber-security with the EU and between member states. To play an important role in shaping cyberspace and cyber-security, the EU cannot treat the internet as simply a communication tool or trading platform. Cooperation and capacity-building measures are needed to allow EU member states to surpass mere coordination of their respective national cyber-security strategies. To succeed as a cyber-power, the EU should adapt new and different forms of cyber-power, from the compulsory through the institutional, to the structural and productive. Otherwise, coordination of national strategies for cyber-security of EU member states is the most the EU as an actor can aim for.

The beginning of the 21st century has seen the emergence of cyber-security as a major issue of international security. [1] While traditional military issues are far from irrelevant, major powers are increasingly preoccupied with the new agenda. When American President Obama and Chinese President Xi met in June 2013 at the informal two-day Sunnylands summit, they talked about traditional regional security issues like North Korea and its nuclear programme, rising concerns like climate change and intellectual property rights, as well as cyber-security and especially cyber espionage. [2]

Policy and research on European cyber-security remains relatively formative. The European Union has been slower to elevate the issue, only recently introducing its *EU Cyber Security Strategy - Open, Safe and Secure.*[3] This was accompanied by a legislative proposal, the *Proposed Directive on Network and Information Security,* from the European Commission to strengthen the security information systems in the EU.[4] Most authors focus on cyber-security and defence policies of big powers, especially China and the United States.[5] Alternatively,

cyber-security is treated as a new and challenging field on its own regardless of national references.

This article evaluates the European Union as a cyber-security actor. Specifically, it asks fundamental questions concerning the EU's combination of prominence and obscurity, especially its limitations and prospects. Who and what is going to dominate the European response to cyber-security in the future? These questions will be examined within the larger framework of liberal intergovernmentalism. The European Union is also compared to the North Atlantic Treaty Organization (NATO), as a point of reference to further understand the limitations and challenges ahead for the EU.

Above all, the European Union suffers from lack of collective vision on cybersecurity. This analysis shows two major factors that limit the European Union as an actor in the field of cyber-security. First and most fundamental is the intergovernmental character of the European Union. At present, the EU is best characterized as a particularly intense form of intergovernmental cooperation, with some pooling and delegating of sovereignty to facilitate common aims and objectives.[6] Second is the fundamental lack of collective vision of cyber-security on the part of the European Union and its member states.

For the EU to play an important role in shaping cyberspace and cyber-security, it cannot treat the internet as simply a communication tool or trading platform. Cooperation and capacity-building measures are needed to allow EU member states to surpass mere coordination of their respective national cyber-security strategies. To succeed as a cyber-power, the EU should adapt new and different forms of cyber-power, from the compulsory through the institutional, to the structural and productive.[7]

Understanding of Cyber-Security: A Lack of Conceptual Clarity?

As Lior Tabansky observes, cyberspace is composed of all the computerized networks in the world, as well as 'end points' that are connected to the network and controlled through it.[8] This space is increasingly accessed by mobile rather than stationary devices. As such, cyberspace is composed of three layers: the infrastructure (physical layer such as storage devices, processors, etc.), software (computer systems and applications that interact with one another), and data held by the machines.[9]

This still not fully explored environment presents fundamental challenges for the conceptualization of cybersecurity. Consequently it is not an easy task to elicit the understanding of cyber-security in the case of the European Union. Many EU member states have their own cyber-security strategies and their own conceptualizations of cyber-security.

The EU as a whole is not entirely clear on the notion. The *EU Cyber Security Strategy - Open, Safe and Secure* does not include a definition of cyber-security. One has to elicit this meaning from publications of the European Union Agency for Network and Information Security (ENISA). [10]

For its own purposes, ENISA defines cyber-security as ' ... 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' .[11] Importantly it includes the basic characteristics of cyberspace: a wholly man-made environment that partly exists in physical form - information hardware (infrastructure of many kinds) and information software (that effectively enables social relations). Part of the understanding of cyber-security in this case relies on threats that emanate from the global environment. These threats are specified as cybercrime, cyber espionage and cyber warfare. [12] This seems rather general and superficial.

Particular EU member states might offer much deeper understandings of cybersecurity specified in the form of national cyber-security strategies. However, according to ENISA data, only 15 EU member states actually have national cyber-security strategies. [13] The remaining 12 do not have dedicated strategies, so they address cyber-security through their respective national security strategies, if at all. Their national narratives differ from case to case. Estonia, one of the most computerized societies, emphasizes the necessity of a secure cyberspace in general and focuses on information systems. Their recommended measures are of a civil character and concentrate on regulation, education, and cooperation.[14] The United Kingdom, on the other hand, in its 2011 document stresses its role as a trade partner:

... concentrating on the national objectives linked to evolving cyber security: making the UK the major economy of innovation, investment and quality in the field of ICT and by this to be able to fully exploit the potential and benefits of cyberspace. The objective is to tackle the risks from cyberspace like cyberattacks from criminals, terrorists and states in order to make it a safe space for citizens and businesses.[15]

Herein lies the fundamental weakness of the European response to cyber threats. There is no coherent European understanding of what the notion of cyber-security should include. Consequently, conceptualization differences are more than likely to produce different approaches to respective national capabilities catalogues. Such inconsistencies, when reinforced by national security narratives and traditional sovereignty claims, are more than likely to leave the EU toothless in the future.

NATO's understanding of cyber-security tends to be narrower, focusing on the functional

aspects of the organization:

The main focus of the NATO Policy on Cyber Defence is on the protection of NATO networks and on cyber defence requirements related to national networks
that NATO relies upon to carry out its core tasks: collective defence and crisis management. [16]

As a military alliance based on collective defence, epitomized by Article 5 of the North Atlantic Treaty, NATO has incorporated thinking about cyber-security mainly in terms of national and collective security. The narrative is more pertinent to traditional security, military based and nationally provided. Such a narrow conceptualization, heavily influenced by the United States, seems more effective for actual capacity-building. The major point is that NATO in its official doctrine links cyber-security to the alliance's fundamental goals: preservation of security of its members and coordinated assistance, should an attack take place. Effectively speaking, that means invoking Article 5.

Coordination *vs* Cooperation: The Structural Limitations of the EU

As a *sui generis* institution, the European Union proves to be a challenge for security experts. It is an actor in international relations, especially since the Lisbon Treaty of 2009 which codified the EU's legal personality. But its agency in foreign policy is often controversial. Developments under the Common Foreign and Security Policy led to the establishment of a range of institutions such as the European Defence Agency, the Helsinki Headline Goal, the European Gendarmerie Force, European Union battle groups, and the European Union Institute for Security Studies. The EU has permanent bodies, such as the Political and Security Committee, the European Union Military Committee, the European Union Military Staff (EUMS), the Committee for Civilian Aspects of Crisis Management, and the European Union Satellite Centre. Additionally, in 2009 the world saw the introduction of the Common Security and Defence Policy (CSDP), formerly known as the European Security and Defence Policy (ESDP). [17] Since 2010, it this been facilitated by the European Union External Action service. [18]

The reality, however, is that cooperation within what was the second pillar (Common Foreign and Security Policy) is essentially intergovernmental. Major decisions of the European Council and the Council of the European Union are taken either by consensus or by unanimity respectively, whereby national narratives hamper a truly common vision from emerging. It is true that the EU leads a number of police and military missions around the world. As of 30 May 2014, these missions include five ongoing military operations and as many as 10 civilian ongoing missions.[19] Given that the first EU mission happened only in 2003, the EU has quite an impressive number of ongoing and completed operations.[20] Quantity, however, does not

necessarily translate into quality, as shown by the recent perturbations with Europe's response to the crises in Libya, Syria, or Ukraine. The strongest of these, tagged by the press as Europe's first war or baptism of fire - the operation in Libya - involved some of the EU's powers but did not prompt civilian or military operations by the whole of the EU for almost two years.[21] Coming just after the creation of the External Action service in 2010, when dealing with EU diplomats, officials of the United States and other countries continued to point to the organizational problems that stemmed from the lack of a 'Mr Europe' .[22]

This account serves as an introduction to further analysis of EU structural frameworks that influence cooperation within cyberspace. For the time being, the EU' s most advanced institution responsible for dealing with cyber-security is ENISA, the European Union Agency for Network and Information Security. Created in 2004, it is located in Heraklion, Crete. As of mid-2014, its objectives were 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'. As such, it serves as an access point for EU member states and other stakeholders.

In that sense, the EU can be conceptualized as an institutional cyber-power, a power that rests on indirect control of one actor's manoeuvring field through third party institutions. The most powerful actors are able to set norms and standards that ultimately shape the environment in which they and all other actors exist and through which they try to arrive at their goals.[23] Consequently, this part of the article will address two elementary avenues for an institution such as the EU to shape its institutional component of cyber-power: international cooperation, and facilitation of member states' approaches to cyber-security threats.

EU as a Global Cooperation Institutional Agent?

When dealing with global security threats and challenges, such as those in the cyber domain, it is almost a cliche to note that the response on the part of national governments needs to cut across traditional lines of organizational structures. The EU Parliament, the Commission and ENISA certainly realize 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 United States. Such cooperation will definitely be easier when it comes to cybercrime, but not when regarding cyber espionage or cyber-attacks, which most states tend to treat as forms of economic competition.

Cooperation between the European Union and the United States developed under the general framework of transatlantic cooperation in cyber-security.24 In particular, the EU - US

Working Group on Cyber-Security and Cyber-Crime has been established.[25] The focus is on organizing events like that on 12 June 2012, devoted to gathering all potential intermediaries together to exchange experiences from both sides.[26] The alliance between these two is vital, as both are 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 experience-sharing, are important, but fundamental problems limit their effectiveness. Four problems stand out. First is the lack of clarity on the institutional side. As mentioned earlier, the NATO Rapid Reaction Team (RRT) focuses more on the American side of the Atlantic. The United States 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.[27] But some EU members, like Greece and Poland, have not.[28] Secondly, there is an essential problem with the lack of a commonly agreed definition of cyber defence among EU members as well as between the EU and the US. Thirdly, as James Lewis and Heather Conley observe, recent lack of progress in effective cyber-security cooperation is coupled with the National Security Agency (NSA) spying revelations that have created an environment of transatlantic uncertainty and distrust. [29]

Finally, there is the question of the International Treaty on Cyberwar. As much as the idea is supported by some EU member states, it gets little support from the American administration. As Richard Clarke concludes, depending on the agreed definition of cyber warfare, a global cyber treaty might limit the United States from carrying out activities like cyber espionage, 'but it is extremely doubtful that some other nations would in fact follow its provisions' .[30] Worse still, the document would have to be channelled through the United Nations, which is notorious for slow responsiveness to pressing threats.

International law itself is outdated, with no clear vision among the international community as to how it should encapsulate cyberwar.[31] As Marry O'Connell observes, existing international law on the use of force is largely irrelevant when it comes to cyberspace since the former is mostly conceived of as space for communications and economic activity.[32] Therefore the relevant law should logically be law on economic rights. By extension, the international law on self-defence and the use of force is not directly applicable to the cyber domain.[33] It is often forgotten that the UN Charter was drafted during a time when the internet was unimaginable, and the most advanced equipment in the realm of computation and information were probably code machines like Enigma, used by Germany during the Second World War, and huge computing machines that took up whole rooms.[34]

As for other major stakeholders, the EU has recently been pursuing the issue, for example in

cyber-security talks with Chinese officials. The Joint Press Communique of the 14th EU-China summit of 14 February 2012 recognizes the importance of 'deepening understanding and trust on cyber issues' .[35] What this means in practice is that China and the European Union will set up a China-EU Cyber Taskforce. The aims of the taskforce seem moderate: addressing 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.[36] Commentators question the effectiveness of the taskforce, pointing to its confidence-building-like function rather than actually reducing cybercrime. [37] The basic problem is that China and the EU have different concepts of cyber-security and the cyber realm in general. The strategic partnership set up in 2003 remains highly declaratory and trade related.[38] Meanwhile, China is identified behind serious acts of cyber espionage against states and private enterprises.[39]

The situation for Russia is similar. Matters of cyber-security (mainly cybercrime) are covered by the Partnership and Cooperation Agreement, especially its Common Space of Freedom, Security and Justice.[40] Yet cooperation between the EU and Russia has flourished due to human rights disputes, such as visa requirements for Russian citizens to travel to EU countries, and difficulties for Russians living in Kaliningrad to reach other parts of Russia, as well as energy and security issues and European cooperation with the United States. Russia has been heavily criticized by Europeans for its involvement in the crisis in Georgia in 2008, its 'unreliable' stance on Libya in 2011, Syria, and most importantly its intervention in Ukraine in 2014. With Putin as President of the Russian Federation, many observers expect the continuation of tensions and limited progress.[41] As for cyber-security issues, Russia is still perceived in Europe with great unease, given its attack on Estonia in 2007, sometimes called the first instance of cyber warfare, which led NATO countries to establish the NATO Cyber Defence Centre in Tallinn.[42]

Coordination of National and Private Stakeholders' Responses in the Case of Cyber-Attacks

As the EU' s prime institution for exchange of information and best practices in information security, ENISA assists member states with their own national cyber-security strategies. For this purpose, a *Good Practice Guide* was finalized in 2012.[43]

The European Commission encourages energy, transport, and financial companies in the EU to invest more in their cyber-security and to report breaches that could compromise their security.[44] Pertinent to the role and significance of 'critical infrastructure', private entities are part of the same system, which can only be as strong as its weakest element.[45] Therefore the

Commission plans to extend security breach notifications to new industries other than telecommunications companies and internet firms, which in Europe are already subject to reporting obligations.[46]

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.[47] 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. In this regard the directive of the European Parliament and 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 largescale attacks against information systems.[48]

One of the most advanced actions to date is the organization of 'Cyber Europe 2014', an exercise claimed to be the biggest European cyber-attack simulation.[49] The scenario revolved around large-scale cyber-incidents that affected all participating countries. Fictional adversaries joined forces for a massive cyber-attack, mainly through Distributed Denial of Service (DDoS) attacks against public electronic services. The affected services were online e-government and financial (e-banking, etc.) services.[50] Just like two exercises in 2010 and 2012, this proved the importance of procedures and points of contact between the member states, trust-building measures and considering the character of the information to be shared in the event of an attack.

NATO as a Platform for Cyber Cooperation

EU institutions tend to act as facilitators of the coordination of national responses, much along the lines of intergovernmentalism.[51] As a military alliance, NATO is based on the clear commitment of its members to collective security and common defence. NATO has greatly incorporated its thinking about cyber-security into its security policy. Two differences stand out that make NATO better suited as a security agent in cyberspace. It understands cyber-security more narrowly than the EU, and much more in relation to the basic functions of the alliance. And it has established its own NATO Computer Incident Response Capability (NCIRC) for day-to-day activity and mitigation measures.

The organization has a clear road map that stipulates practical steps to be taken as well as concrete commitments by its members to build real cyber defence capabilities. The NATO Action Plan is strategic in its approach to building real capacity, inasmuch as it is supposed to be adaptive and goal oriented. In practical terms this means that NATO has embarked on the

creation of minimum requirements for those national information systems that are critical for carrying out NATO's core tasks: assisting allies in achieving a minimum level of cyber defence in order to reduce vulnerabilities to national critical infrastructure; fully integrating cyber defence into the NATO Defence Planning Process; defining cyber defence requirements for non-NATO troop-contributing nations; enhancing early warning, situational awareness, and analysis capabilities; and finally, encouraging NATO and allies to draw on expertise and support from the Cooperative Cyber Defence Centre of Excellence in Tallinn.[52] The two cyber defence activities that top the list, as defined by the Alliance, are assisting individual allies and integrating cyber defence into their Defence Planning Process.[53] The former focuses mainly on protecting the communication systems owned and operated by the Alliance. National critical infrastructure is still protected at the national level; NATO declares its readiness to assist its members in building up much-needed resources but also requires them to provide and maintain a reliable and secure supporting infrastructure. This means that national and Alliance cyber defence planning activities are to be harmonized to meet agreed targets. Additionally, cyber defence has been integrated into the Alliance's Smart Defence initiative, whih is based on the logics of synergy and is designed to streamline the process of developing capabilities that would not be possible to achieve alone.

In 2007, Estonia experienced a cyber-attack that briefly affected much of the Estonian population, and caused tangible economic losses such as Estonia Hansbank' s reported loss of over USD 1 million.[54] This was a wakeup call that compelled states to treat cyberspace in strategic terms. [55] Partly in consequence, Estonia hosts the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn. The centre is responsible for exercises that allow the participants to test skills to fend off a real attack.[56] The 'Locked Shields' exercise involves governmental and non-governmental aid organizations in an imagined country facing an insurgency that is targeting their IT systems.[57] The CCDCOE's wideranging responsibilities also include contributing to development of cyber defence practices and standards with NATO, its members, candidate and Partnership for Peace countries, and contributing to development of NATO policies on cyber defence.[58] *The Tallinn Manual on the International Law Applicable to Cyber Warfare* is the Centre's most acclaimed publication, focused in particular on the international law relevant to this field. [59]

NATO, as a military alliance, defines cyber-security in a narrow way that relates mainly to its basic roles. The Alliance also focuses more on creation of real cyber capabilities and a feasible road map. Its role is more to facilitate cooperation and interoperability, compared to that of the European Union, which is mainly a facilitator of intergovernmental coordination.

Defensive *vs* Offensive Capabilities: The Functional Character of the EU

Students of European integration and its institutional emanation are often presented with a picture of the EU as a civilian power. As summarized by John McCormick, Europe now sees itself - and is mainly seen by others - as a civilian power. It poses a military threat to no one; it faces no immediate conventional military threats of its own, and it does not feel the need to use force or the threat of force to encourage change; instead, it offers the incentive of opportunities.[60]

Reconciling this with ever-changing security challenges is a major test. Cyberspace, a great emancipator for non-state actors, also challenges the EU's civilian character. With some of the most advanced countries in the world and a huge market, much is at stake in the EU's cyber-security. For example, in March-April 2011, European Commission IT experts detected an intrusion in their systems - an attack against the European Union's Emissions Trading Scheme which saw at least EUR 30 million of emissions allowances stolen from national registries. [61]

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 private agents acting regardless of political agenda. The usual targets are private citizens and businesses. Threats in this category are usually referred to as cybercrime or computer crime. Most often, the aim of the perpetrators is to acquire information such as the private data of customers. The second category, by contrast, involves political motives such as power maximization, advantage or disadvantage creation and so on, and hence involves states or other non-state but politically motivated actors, such as terrorist organizations. Threats under this category include cyber espionage, cyber terrorism, or threats against critical infrastructure.[62]

European experts and decision-makers have been calling for better institutional responses to both sets of threats. According to Brussels, worldwide more than one million people become victims of cybercrime every day. The cost of cybercrime has been estimated at USD 388 billion globally.[63] By 2011, nearly three-quarters (73 per cent) of European households had home internet access, and in 2010 more than one-third of EU citizens (36 per cent) were banking online.[64] 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 one Euro per card, a counterfeited physical credit card for around EUR 140 and bank credentials for as little as EUR 60.[65] A study by the security firms Guardian Analytics and McAfee found that Europe is the primary target for cybercrime-related activity such as Zeus and SpyEye tactics, bypasses for physical multi-factor authentication, automated mule account databases, as well as server-based

fraudulent transactions. [66] Because of the nature of network infrastructure, attacks may include a number of institutions based in various countries, which adds to the complexity that national Computer Emergency Response Teams (CERTs) face. National responses are not sufficient.

With these problems in mind, under the Digital Agenda for Europe, adopted in May 2010, the Commission committed itself to establishing a CERT for EU institutions, as part of the EU's commitment to a reinforced and high-level EU Networking and Information Security Policy in Europe. Consequently, in September 2012 the EU set up its own permanent Computer Emergency Response Team (CERT-EU) for EU institutions.[67] CERT-EU is defensive, which considerably limits the EU's leverage in cyberspace:

CERT-EU's mission is to support the European Institutions to protect themselves against intentional and malicious attacks that would hamper the integrity of their IT assets and harm the interests of the EU. The scope of CERT-EU's activities covers prevention, detection, response and recovery.[68]

From a legal standpoint, effective cybercrime management requires harmonization of legal, regulatory, and technical provisions concerning the protection of personal data, privacy, and the interests of legal persons.[69] The EU has its own European Cybercrime Centre (EC3), attached to Europol. It is a small unit (around 30 staff) that coordinates cross-border law enforcement and acts as a centre for sharing of technological expertise.[70] Its official activities include support to member states and the European Union's institutions in future building of the capabilities required to coordinate activities addressing cybercrime. It remains to be seen how effective it can be. Since EC3 only commenced operations on 1 January 2013, it is difficult to evaluate or compare it to the general aims of EU cybersecurity. [71]

NATO's response to cyber-security threats revolves around two major notions: prevention and resilience. The latter is understood as facilitating fast recovery once an attack actually takes place, and so logically speaking, it falls into the area of post-event reaction. The former, however, is by definition based on attempts directed at reducing or even deterring those who are behind the threats and is so designed to maintain a certain level of security. By its nature, prevention takes place continually and relies on tangible capabilities that suggest 'imminent and unavoidable' response of a retaliatory character. When NATO, even if only in its doctrine, incorporates Article 5 into its collective security response, it serves as a deterrent of its own kind. Given the 'attribution problem' that notoriously plagues the cyber domain, this is less likely and therefore remains a last resort. The looming threat of Article 5 is also likely to incentivize the perpetrators to refine their techniques and remain unidentified or, even better,

unnoticed.

It seems that countries and organizations face growing pressure under these circumstances to tum to proactive (pre-emptive) operations. The idea of proactive cyber defence stems from American thinking about information warfare after the end of the Cold War. It is based on much older concepts of 'fore-knowledge', prominently featured in the writings of such classics as Sun Tzu's *Art of War.* As Richard Colbaugh and Kristin Glass put it, 'cyber security researchers and practitioners are focusing their efforts on developing proactive methods of cyber defence, in which future attack strategies are anticipated and these insights are incorporated into defence 'designs'.[72] These ideas revolve around increasing the ability of defence systems to predict new attacker behaviour and reducing their capacity to anticipate defensive actions.

Let us again take a look at NATO. Its 2010 Strategic Concept *Active Engagement, Modern Defence* gives explicit recognition to cyber threats to national securities of NATO members and the Alliance itself. Much along the lines of proactive operations, the document identifies developing abilities to prevent, detect, and defend against cyber-attacks as part of its deterrence and defence mission.[73] In practical terms, NATO started planning a cyber defence programme. It envisaged creation of the Computer Incident Response Capability, which became fully operational in 2012.[74] Becoming proactive means that as a military alliance, NATO will develop minimum requirements for those national information systems that are critical for carrying out NATO's core tasks: assisting allies and other countries in achieving a minimum level of cyber defence to reduce the vulnerabilities to national critical infrastructure; offering help to any of its members should they find themselves a target of a cyber-attack; and enhancing early warning, situational awareness, and analysis capabilities.[75]

Unlike the European Union and its rather reactive/defensive approach, based mainly on coordination between national Computer Incidents Response Teams (CITRs), NATO aims at becoming a proactive agent of cyber-security that operates alongside its member states and even sets benchmarks for member states to meet. Its stance is more than defensive, which emanates from its organizational structure and functional character.

Brave New (Uncertain) World: New Threats and Old Responses

After months of preparatory work, the EU finally released its *Cyber Security Strategy* in February 2013. Subtitled *Open, Safe and Secure,* it is essentially reactive, stressing a free and open internet, understood as the backbone of economic growth. [76] The document, which is for political reference only, stipulates six strategic priorities and actions: achieving cyber resilience; drastically reducing cybercrime; developing a cyber defence policy and

capabilities related to the framework of the CSDP; developing industrial and technological resources for cyber-security; establishing a coherent international cyberspace policy for the EU; and promoting EU core values.[77]

It appears that the major tools as envisaged by this strategy are: public-private partnership, which includes cooperation with industry and academia; developing legislation on cybercrime; and increasing critical infrastructure resilience. This requires implementation of a broad amount of legislative instruments in the coming years. The bottom line seems to be summarized by Action No. 29, as stipulated by the *Digital Agenda for Europe - A Europe 2020 Initiative,* as combating cyber-attacks against information systems.[78] The EU response is understood as requiring

Member States to amend their criminal laws regarding attacks against information systems. The main aim is to provide EU law enforcement authorities with enhanced tools to fight cybercrime. It will include provisions for the use of specific software ('Botnets') as a method of comm1ttmg cybercrimes, making it a criminal offence and also increasing the maximum penalty for offenders. [79]

The most interesting and yet unclear development (also in terms of academic research) is cyber defence policy and capabilities related to the framework of the CSDP. It remains to be seen what these declarations develop into in terms of real action plans and capabilities. New threats have the potential of facilitating CFSP cooperation beyond mere coordination. Since the nature of cyberspace makes traditional intergovernmental arrangements based on national sovereignty less effective, more could be achieved in the realm of cyber defence than has been gained so far in the four traditional domains of air, land, sea, and space.

Since cyberspace is by definition trans-border and transnational, any effective response should also evoke trans-border and transnational cooperation. At the same time, the cyber domain differs from other realms in that it is, partly at least, not physical. What is physical (mainly computer hardware) tends to be much cheaper in terms of Research and Development (R&D) and maintenance than traditional military equipment. Also, the IT know-how seems to be much more evenly spread between countries than, say, anti-ballistic missile technology. Much more than Justice and Home Affairs (JHA), moreover, cyberspace knows no national border.

For the time being, however, the EU remains only a centre of coordination of some aspects of national digital security strategies. It focuses more on the safety of individuals and private companies or operators of critical infrastructure. 80 The next section of the article will

elaborate on the possible solutions, listing five specific prescriptions.

Conclusion: The Way **Forward amid Limitations and Uncertainties?**

It seems likely that particular member states will dominate European action on cybersecurity challenges over a genuine common response. Major reasons start with the lack of a common definition of cyber-security among EU members, which spreads to further conceptual differences regarding related notions such as cyber-power, cyber defence and cyber-security strategy. On a more practical level it translates into problems with interoperability between various national cyber-security institutions as well as a lack of common understanding regarding the role of the state in cyber-security and by extension public-private partnership.

As Doug Stokes and Richard Whitman observe, 'Despite achievements that were unthinkable in the early post-Cold War years, the EU today fails to punch its true weight and to capitalize on its strengths. Why is this still the case?' [81] Two reasons are seen as pervasive: first, the lack of joined global policy whereby multilateral objectives are not effectively translated to bilateral partnerships, and vice versa; and second, the existing differences between member states regarding their relations with emerging powers. The European Union for all its achievements is still only a model of pooled sovereignty, more advanced in some areas than others. The execution of foreign and security policy is especially problematic, as this area still operates on an intergovernmental logic, which will continue in the coming years.

These same general weaknesses feature in EU cyber-security strategy. Behind this state of affairs is the lack of a truly pan-European vision of the role of the EU as an agent of cyber-security on the part of particular member states as well as the whole institution. What limits the European Union most in cyber-security is its intergovernmental character and the corresponding lack of collective vision on the part of member states.

Today, national authorities often seem committed to closer cooperation within the cyber domain, but in reality their commitment is limited and focused mainly on trade and communication-related aspects of cyber-security. The situation bears close resemblance to typical problems in the area of freedom, security, and justice (Justice and Home Affairs). Beginning with cooperation under the Trevi process, later reinforced by the Treaty of Maastricht, obstruction by national authorities was seen when it came to sharing sensitive information and touching directly on national sovereignty concerns.[82] Much of the JHA area, from the outset, was complex, overburdened with national agencies and different national civil laws.

When implementing the EU *Cyber Security Strategy,* five major problems have to be resolved.

Firstly, international cooperation, especially when referring to cyber espionage, is likely to be disappointing for the simple reasons of divergent interests and competition between states. In that sense, coordination of national strategies for the cyber-security of its member states may be the most the EU can aim for in the short term. But regional cooperation should be feasible, since all EU member states belong to the same security community and share a significant convergence of interests. By the same token, meaningful cooperation with key partners such as the United States or Israel should be attainable and politically desired. Growing tensions in international relations, especially with China and Russia, or the protraction of problems in the Middle East, encourage international cooperation in the West.

Secondly, technology does change the balance of power between and within states. In that respect, the internet, just like the printing press before it, provides easy access to information, creating huge pressure on those who govern. Technological developments and communication liberalization empower individuals and private entities, which can provide states with an 'extra hand' in their fight against cybercrime or the protection of critical infrastructure. By the same token, individuals can engage themselves against states and realize real damages to financial or critical infrastructure, disproportionate to the perpetrator's costs, size, or political eminence. As John Sheldon observes, cyberspace is different from all its technological predecessors. Apart from constituting a means of communication, it is also - and perhaps most importantly - a predominant form of creating, storing, modifying, and exploiting information.[83]

Thirdly, the future EU cyber-security strategy should incorporate different forms of cyber-power, from compulsory through institutional, to structural and productive. Only a balanced combination of all four forms will allow a truly strategic approach. Europeans need to understand that the creeping threats to cyber-security continue to affect not only the security of their states but also the security of the whole EU, especially if it expects to be an important actor.

Fourthly, as Ronald Deibert, Rafal Rohozinski and Masashi Crete-Nishihara note in their study of the 2008 Georgia - Russia conflict, control of the physical infrastructure of cyberspace is critical strategically and tactically. [84] For European countries this is challenging because in free-market economies the role of the state, though varying from economy to economy, is limited. As Colin Crouch observes, contemporary Wes tern societies face the post-democracy phenomenon. [85] It is characterized by the withdrawal of the state from most of its functions and thus opening public goods, such as security, to private actors.[86] This creates pressure for EU policymakers to decisively define the role of the state and the EU in cyber-security. Thiswould probably mean 'Brusselization', often opposed by national

governments. However, if the EU is to play a more prominent role in cyber-security in the future, there is probably no alternative. Consequently, private operators will also have to follow more detailed legislation that would stipulate their responsibilities in cases of security breaches (especially in case of Critical Infrastructure and cybercrime).

Finally, EU cyber-security strategy needs to clarify what is actually meant by cyber-security or cyber-security strategy. Contemporary understandings from ENISA seem to be sweeping and general, a challenge to developing operational capabilities. EU cyber-security strategy needs more than merely coordination of national actions. What is needed is supra-natural understanding of challenges and threats and the feasible tools to address them. Such an approach would further Europeanize state security policies, perhaps with the help of the spill-over that characterized European integration for so long. Similarly to the public-private partnership problems mentioned above, it is expected that there will emerge brakemen to any attempts at making concepts uniform. Perhaps, as in other policy areas, the EU will be the scene of a clash of interests between the drivers and brakemen. It is, however, also possible that the character of the cyber domain and threats to cyber-security will make a common response based on common concepts easier in the long run than, say, striking the balance between agricultural and cohesion policies.

The question of agency in the fifth domain has been usefully approached by Stuart Starr, who, referring to American cyber-security strategy, postulates that cyber-power should be seen as the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power, especially military and informational levers of power.[87] We can debate the means that American decision-makers chose when designing their national cyber-security strategy. Equally, we should perhaps argue about their definition of cyberspace, cyber-power or cyber strategy. No one can deny, however, that the United State's agency in cyber domain is undeniable.

Analysing the EU and its cyber-security strategy, one naturally remains skeptical about EU agency in the cyber domain. The EU as a civilian power tends to focus on defensive rather than offensive elements of cyber-security in its approach and so its capacity to truly influence the myriad of actors and phenomena in the cyber domain remains limited. Correspondingly, the comparative underdevelopment of Common Foreign and Security Policy that stems from the intergovernmental character of the EU in this regard fixes it on civilian elements of cyber-security such as those relating to trade and communication. Unlike NATO, the European Union does not instil cooperation based on well-defined, focused, military-related functionality; it merely encourages generic coordination. In this respect the ENISA *Good Practice Guide on National Cyber Security Strategies* to broadly coordinate national

cybersecurity strategies is only a first step on the long road that lies ahead.[88]

NOTES

1. Myriam Dunn Cavelty, 'Is Anything Ever New? Exploring the Specificities of Security and Governance in the Information Age', in Myriam D. Cavelty, Victor Mauer, and Sai-F.K. Hensel (eds), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace* (Aldershot: Ashgate, 2007), p. 19. For an overview of cyberspace definition, see Daniel T. Kuehl, 'From Cyberspace to Cyberpower: Defining the Problem', in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (eds), *Cyberpower and National Security* (Washington, DC: Center for Technology and National Security Policy, 2009), pp. 26-8.

2. 'Remarks by President Obama and President Xi Jinping of the People's Republic of China after Bilateral Meeting' (Sunnylands Retreat, Rancho Mirage, California), The White House Office of the Press Secretary, 8 June 2013.

3. *EU Cyber Security Strategy - Open, Safe and Secure* (Brussels: European Union, 2013).

4. *Proposed Directive on Network and Information Security* (Brussels: European Union, 7 February 2013). As of 30 May 2014 the document was still awaiting Council first reading position/budgetary conciliation convocation.

5. Richard A. Clarke and Robert K. Knake, *The Next Threat to National Security and What to Do About It* (London: HarperCollins Publishers, 2010); Kramer, Starr, and Wentz, *Cyberpower and National Security* (note 1). For China and the US, see Kenneth Lieberthal and Peter W. Singer, *Cybersecurity and US-China Relations* (Washington, DC: John L. Thornton China Center at Brookings, 2012). General studies worth recommending include David Betz and Tim Stevens, *Cyberpower and the State: Toward a Strategy for Cyber Power* (Routledge: The International Institute for Strategic Studies, 2011) at http://www.academia.edu/l150127/Cyberspace_and_the_State_Toward_a_Strategy_for_Cyber-Power, and Jan-Frederik Kremer and Benedikt Miiller (eds), *Cyberspace and International Relations: Theory, Prospects and Challenges* (Berlin: Springer, 2014).

6. Simon Bromley (ed.), *Governing the European Union* (London: Sage Publications in association with the Open University, 2001), p. 70.

7. Betz and Stevens, *Cyberpower and the State* (note 5).

8. Lior Tabansky, 'Basic Concepts in Cyber Warfare', *Military and Strategic Affairs,* Vol. 3,

No. 1 (May 2011), p. 77.

9. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), pp. 12-13.

10. See http://www.enisa.europa.eu/ (accessed 30 May 2014).

11. Udo Helmbrecht, Steve Purser, and Maj Ritter Klejnstrup, *Cyber Security: Future Challenges and Opportunities* (Heraklion: ENISA, 2012), p. 13.

12. *Ibid.,* pp. 12, 13.

13. *Cyber Security Strategies in the World* (Heraklion: ENISA, n.d.).

14. *National Cyber Security Strategies. Setting the Course for National Efforts to Strengthen Security in Cyberspace* (Heraklion: ENISA, 2012), p. 5.
15. *Ibid.,* p. 6. See also *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (London: Cabinet Office, November 2011), p. 23.

16. *Defending the Networks: The NATO Policy on Cyber Defence* (Brussels: North Atlantic Treaty Organization, 19 August 2011).

17. Common Foreign and Security Policy (CFSP) of the European Union, at http://eeas.europa.eu/cfsp/ accessed 30 May 2014).

18. European Union External Action, at http://www.eeas.europa.eu/index_en.htm (accessed 30 May 2014).

19. European Union External Action, 'Ongoing Missions and Operations', at http://www.eeas.europa.eu/csdp/missions-and-operations/index_en.htm (accessed 30 May 2014).

20. As of23 May 2014, the EU has completed 10 civilian missions and five military operations. See European Union External Action, 'Ongoing Missions and Operations' (note 19).

21. In fact, EU member states such as France and the United Kingdom that did take part in military intervention in Libya did so under respective national engagements. Interestingly,

Canada, France, the United Kingdom, and the United States had their own code names for the operation. See 'France: Libya War Marks New Chapter in EU-US Relations', at http://euobserver.com/defence/113486, 1 September 2011.

22. Looking at the way EU diplomats behave outside the EU, a veteran diplomat from one member state told euobserver: 'What you see in the big emerging countries and in the US, is that each [EU] country defends its privileged relationship. When you talk to the Chinese or to the Indians they say: "Yes, we have this EU summit once a year. But for the rest of the time, each of your countries comes and says the EU is not important"'. See more at 'EU Ponders Creation of New Diplomatic Breed', at http://euobserver.com/institutional/30209, 4 June 2010.

23. Betz and Stevens, *Cyberspace and the State* (note 5), p. 47.

24. Until 2010, when the US and EU held regular exercises on cyber defence, there has been no effective formal cooperation between the two. The US had cooperated on an informal, bilateral basis with some EU member states in the areas of cybercrime and information-sharing for the purpose of prevention and sharing. For more information, see Michael Vatis, 'International Cyber-Security Cooperation', in James A. Lewis (ed.), *Cyber Security. Turning National Solutions into International Cooperation* (Washington: The CSIS Press, 2003), p. 9.

25. 'Cyber Security: EU and US Strengthen Transatlantic Cooperation in Face of Mounting Global CyberSecurity and Cyber-Crime Threats', Europa Press Release, 14 April 2011, at http://europa.eu/rapid/pressReleasesAction.do?reference=MEM0/111246 (accessed 30 May 2014).

26. See more at 'EU-US Event on Intermediaries in Cybersecurity Awareness Raising', ENISA, at http://www.enisa.europa.eu/activities/cert/security-month/eu-us-event-on-intermediaries-in-cyber-securityawareness-raising (accessed 30 May 2014).

27. The most important provisions of the Convention are covered by chapter 3, which pays special attention to instruments for international cooperation. For an overview analysis of the Convention on Cybercrime, see Rutger Leukfeld and Wouter Stol, *Cyber Safety: An Introduction* (The Hague: Eleven International Publishing, 2012), p. 65.

28. As of 30 May 2014. See *Convention on Cybercrime CETS No.: 185* (Brussels: Council of

Europe Treaty Office, 2014).

29. James A. Lewis and Heather A. Conley, 'Liberty. Equality, Connectivity - Transatlantic Cooperation on Cybersecurity Norms', A Report of the CSIS Strategic Technology and Europe Programs, Center for Strategic and International Studies, Washington, DC, January 2014, p. 30.

30. Richard A. Clarke and Robert K. Knake, *The Next Threat to National Security and What to Do About It* (note 5), p. 235.

31. Nat Katin-Borland, 'Cyberwar: A Real and Growing Threat', in Sean S. Costigan and Jake Perry (eds), *Cyberspaces and Global Affairs* (Farnham: Ashgate, 2012), p. 17.

32. Marry E. O'Connell, 'Cyber Security without Cyber War', *Journal of Conflict & Security Law,* Vol. 17, No. 2 (2012), p. 199.

33. On the last point, Dimitrios Delibasis presents an interesting view claiming that particular actions should be judged as the violation of fundamental rules of International Relations (IR) not only according to the means but more importantly according to their consequences. See Dimitrios Delibasis, 'Information Warfare Operations within the Concept of Individual Self-Defence', in Athin Karatzogianni (ed.), *Cyber Conflict and Global Politics* (London: Routledge, 2009), p. 98.

34. See more at Edmund Callis Berkeley, *Giant Brains; or, Machines that Think* (New York: Wiley, 1949).

35. *Joint Press Communique of the 14th EU-China Summit* (Brussels: Council of the European Union, 14 February 2012).

36. Zhongqi Pan, 'After the China-EU Summit: Reaffirming a Comprehensive Strategic Partnership', European Strategic Partnership Observatory, Policy Brief 3, April 2012, p. 3.

37. Franz-Stefan Gady, 'China-EU Cooperation on Combatting Cybercrime: A Model for China-US Relations?', China-US Focus, 24 April 2014.

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

39. See Timothy L. Thomas, 'Google Confronts China's "Three Warfares"', *Parameters* (Summer 2010), pp. 101-13.

40. For more details, see EUR-Lex, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:21997All28(01):EN:NOT (accessed 30 May 2014).

41. On the EU-Russia summit in St Petersburg, 3-4 June 2012, see *EU-Russia Summit (St. Petersburg, 314 June 2012),* Europa Press Release, Brussels, 1June2012, at http://europa.eu/rapid/press-release_MEM0-12-40 l_en.htm ?locale=en

42. Mite Valentinas, 'Estonia: Attacks Seen as First Case of "Cyberwar"', Radio Free Europe/Radio Liberty, 30 May 2007.

43. *Good Practice Guide on National Cyber Security Strategies* (Heraklion: ENISA, April 2013).

44. On 14 March 2014, the European Parliament voted on the proposed Network and Information Security (NIS) Directive. The final text of the directive still has to be negotiated between EU law-making institutions, which means that the new law might be ready in 2015 at the earliest. See more at http://www.europar 1. europa. eu/ sides/ getDoc .do ?type= REPORT &reference=A 7-2014-0103 &language= EN (accessed 30 May 2014).

45. In 2008 the Commission established the European Programme for Critical Infrastructure Protection (EPCIP), which described the EU's overall approach to securing Critical Infrastructure (CI). The EPCIP's framework included procedures for identifying and designating European CI and supports member states in their respective activities concerning the protection of national CI. It did not, however, at that stage require operators within member states to report significant breaches of security or facilitate cooperation between member states. See Scott J. Shackelford and Amanda N. Craig, 'Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity', *Stanford Journal of International Law* (Winter 2014), p. 14.

46. 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 of the European Union, 31 July 2002).

47. 'Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks against Information Systems', Official Journal of the European Union, 24 February 2005.

48. *Directive 2013140/EU of the European Parliament and of the Council on Attacks against Information Systems and Repealing Council Framework Decision 20051222/JHA* (Brussels: European Union, 2010).

49. *Biggest EU Cyber Security Exercise to Date: Cyber Europe 2014 Taking Place Today* (Heraklion: ENISA, 28 April 2014).

50. *Ibid.,* p. 5.

51. In its latest report on EU cyber-security, ENISA boasts about its latest achievements: (1) managing Europe's biggest ever cyber-security exercise, Cyber Europe 2012, involving all EU member states and countries from the European Free Trade Area (EFTA); (2) taking a formal role in Europe's Cyber Incident Reporting framework, under Article 13a of the EU's Telecommunications Framework Regulation; (3) responding quickly and efficiently to member states' requests for assistance, through ENISA' s Athens-based Mobile Assistance Team (MAT); (4) helping to establish new Computer Emergency Response Teams (CERTs) in Malta, Romania, Cyprus, and Ireland, as well as ongoing support to established teams. For more details, see *EU Cyber Cooperation: The Digital Frontline* (Heraklion: ENISA, 2012), p. 5.

52. *Defending the Networks* (note 16).

53. *NATO and Cyber Defence* (Brussels: North Atlantic Treaty Organization, n.d.).

54. See Valentinas, 'Estonia' (note 42).

55. Salma Shaheen, 'Offence-Defence Balance in Cyber Warfare', in Kremer and Muller, *Cyberspace and International Relations* (note 5), p. 81.

56. *Cyber Defence Exercises* (Tallinn: NATO Cooperative Cyber Defence Centre for Excellence, n.d.).

57. *International Cyber Defence Exercise Locked Shields 2014 Begins Today* (Tallinn: NATO

Cooperative Cyber Defence Centre for Excellence, n.d.).

58. *Ibid.*

59. *The Tallinn Manual on the International Law Applicable to Cyber Waifare* (Cambridge: Cambridge University Press, 2013); see also Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution', *Journal of Conflict and International Law,* Vol. 17, No. 2 (2012), pp. 229-44.

60. John McCormick, *Europeanism* (Houndmills: Palgrave Macmillan, 2010), p. 200.

61. *Cyber Security: EU Prepares to Set up Computer Emergency Response Team for EU Institutions* (Brussels: European Union, 10 June 2011).

62. See James A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats* (Washington, DC: Center for Strategic and International Studies, December 2002).

63. 'An EU Cybercrime Centre to Fight Online Criminals and Protect e-Consumers, European Commission', Press Release, European Union, Brussels, 28 March 2012, at http://europa.eu/rapid/pressrelease_IP-12-317 en.htm

64. *Ibid.*

65. Such claims should be kept in a 'sober' perspective, however. As Jerry Brito and Tate Watkins demonstrate, the alarmist lines flowing from the cyber-security establishment very often lack clear evidence and therefore are likely aimed at threat creation amid rising national security budgets. See Jerry Brito and Tate Watkins, 'Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy', Working Paper No. 11-24, Mercatus Center, George Mason University, Fairfax, VA, April 2011.

66. Dave Marcus and Ryan Sherstobitoff, 'Dissecting Operation High Roller', White Paper, 2012, at http://www.mcafee.com/uk/resources/reports/rp-operation-high-roller.pdf. McAfee An Intel Company, Mission College Boulevard, Santa Clara. 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.

67. The team is made up of IT security experts from the main EU Institutions (European

Commission, General Secretariat of the Council, European Parliament, Committee of the Regions, Economic and Social Committee). It cooperates closely with other CERTs in the member states and beyond as well as with specialized IT security companies. *About Us* (Heraklion: ENISA, Computer Emergency Response Team (CERT-EU), n.d.).

68. Computer Emergency Response Team, at http://cert.europa.eu/static/RFC2350/RFC2350.pdf (accessed 30 May 2014).

69. Sylvia Mercado Kierkegaard, 'EU Tackles Cybercrime', in Lech Janczewski and Andrew Colarik (eds), *Cyber Waifare and Cyber Terrorism* (Hershey: Information Science Reference, 2008) p. 427.

70. Europol, European Cybercrime Centre (EC3), at https://www.europol.europa.eu/content/megamenu/european-cybercrime-centre-ec3-1837 (accessed 30 May 2014).

71. EC3 has published its first report in which it tries to self-evaluate and present its achievements. The reading, however, turns out to be very short and superficial. See more at https://www.europol.europa.eu/sites/default/files/publications/ec3_first_year_report.pdf (accessed 3 July 2014).

72. Richard Colbaugh and Kristin Glass, *Proactive Defence for Evolving Cyber Threats, Sandia Report* (Albuquerque: Sandia National Laboratories, 2012), p. 91.

73. *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted by Heads of State and Government in Lisbon* (Lisbon: North Atlantic Treaty Organization, 19 November 2010).

74. *Briefing. Tackling New Security Challenges* (Brussels: North Atlantic Treaty Organization, 2012).

75. *Defending the Networks* (note 16).

76. *EU Cyber Security Strategy* (note 3).

77. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', Brussels, 7 February 2013.

78. *Digital Agenda for Europe, Action 29: Combat Cyber-Attacks against Information Systems* (Brussels: European Council, 22 July 2013).

79. In August 2013 the European Parliament and the Council adopted 'Directive 2013/40/EU on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA' *(Official Journal of the European Union,* 14 August 2013).

80. Nathan D. Taylor and Miriam H. Wugmeister, 'Cybersecurity Developments in the US and the EU', Morrison & Foerster Client Alert, 19 February 2013.

81. Doug Stokes and Richard G. Whitman, 'Transatlantic Triage? European and UK "Grand Strategy" after the US Rebalance to Asia', *International Affairs,* Vol. 89, No. 5 (2013), p. 1102.

82. Neil Nugent, *The Government and Politics of the European Union,* 7th edition (Houndmills: Palgrave Macmillan, 2010), pp. 335-336.

83. John B. Sheldon, 'Deciphering Cyberpower. Strategic Purpose in Peace and War', *Strategic Studies Quarterly* (Summer 2011), p. 101.

84. Ronald J. Deibert, Rafa! Rohozinski and Masashi Crete-Nishihata, 'Cyclones in Cyberspace: Information Sharing and Denial in the 2008 Russia-Georgia War', *Security Dialogue,* Vol. 43, No. 1 (2012), p. 17.

85. Colin Crouch, *Post-Democracy* (Cambridge: Polity, 2004).

86. There is now a large body of literature on the phenomenon of 'privatization of security'. In the case of cyberspace the problem is even more evident, since most of the providers are private companies.

87. Stuart H. Starr, 'Toward a Preliminary Theory of Cyberpower', in Kramer, Starr, and Wentz, *Cyberpower and National Security* (note 1), p. 48.

88. Since ENISA remains only an advisory institution within the EU organizational infrastructure and is overseen by a management board composed of representatives from the EU member states, the European Commission, and stakeholders from the information and communication technologies industry, as well as consumer groups and academic experts, its

real influence over the shape and speed of European response to cyber threats remains very limited.