European Security and Defence Forum Workshop

A New European Security Architecture?

Cyber security: European strategies and prospects for global cooperation

Marco Davì
Research Fellow, Carnegie Europe
Carnegie Endowment for International Peace

11 November 2010

This paper was presented at the European Security and Defence Forum (ESDF) organized by Chatham House. Chatham House is not responsible for the content of this paper.

The views expressed in this document are the sole responsibility of the author(s) and do not necessarily reflect the view of Chatham House, its staff, associates or Council. Chatham House is independent and owes no allegiance to any government or to any political body. It does not take institutional positions on policy issues. This document is issued on the understanding that if any extract is used, the author(s)/ speaker(s) and Chatham House should be credited, preferably with the date of the publication or details of the event. Where this document refers to or reports statements made by speakers at an event every effort has been made to provide a fair representation of their views and opinions, but the ultimate responsibility for accuracy lies with this document’s author(s). The published text of speeches and presentations may differ from delivery.
INTRODUCTION

The XXI century security environment is increasingly being characterized by the emergence of new security challenges, inherent systemic risks and simultaneous interplay of qualitatively different actors, capable of affecting a variety of sectors beyond the strictly military dimension at multiple levels of scale (Cerny, 2000). The cyber domain, perhaps better than any other dimension of the global commons, quintessentially embodies the complex uncertainties of contemporary security (Rasmussen, 2006). In fact, the relatively low capabilities required to enter the domain, the operational anonymity, and the vulnerability asymmetry mean that a plurality of actors can exercise hard and soft power in cyber space compared to traditional strategic domains, contributing to the diffusion of power and of security threats in world politics (Nye, 2010). Cyber space has therefore increasingly gained prominence in security thinking and acquired a fundamental strategic importance for policy-making.

At present, cyber warfare is firmly on the international security agenda, while major players are adapting their respective defense structures to address digital risks and threats (Cornish, Hughes, and Livingstone, 2009). In fact, in an increasingly interconnected and interdependent world, in which the future battlefield is likely to be “contested, congested, cluttered, connected, constrained”, the emergence of threats in and from cyber space (Deibert and Rohozinski, 2010) is compelling a fundamental adaptation of the terms of the strategic debate underpinning the formulation of policy responses. Cyber conflict undoubtedly represents a strategic question challenging traditional security concepts, that need to be adjusted for the cyber environment through review and discussion at the national, regional and international levels.

The cyber realm presents a fascinating complexity, as its security significance unfolds across the military, economic, political, societal dimensions. It further interconnects the action scale - from the societal to the global level - of a wide range of actors including individuals, organized groups, and states (Deibert and Rohozinski, 2010). Moreover, its criticality derives from the progressive strategic over-reliance on information technology, rooted in the net-centric warfare and RMA paradigms. Such “network dependence” has become a source of vulnerability, targeted asymmetrically with minimal capabilities inflicting extensive damage that compel nevertheless costly surveillance and defense (Lynn, 2010). Furthermore, the threat’s profile in the cyber realm decidedly blurs the definition of armed attack, complicates the plausibility of attribution and ultimately constrains the role of deterrence for strategic stability. Denial-of-benefit, as opposed to countervalue retaliatory postures, constitutes the only realistic expression of deterrence, given the current state of technology (Lynn, 2010). Consequently, the panoply of policy responses that can prove to be effective appears limited to a set of measures aimed at ensuring the functional security of the network, by increasing its operational resilience and protecting its physical infrastructure.
In seeking to stimulate the debate in such sphere, this paper addresses the specific aspect of emerging cyber security policy and of potential alternatives for cooperative options to manage cyber risk. In light of the structural character of the cyber strategic domain, and of its implications for concepts such as offense/defense, deterrence, and discrimination, to which degree is the current trend in security policy proving adequate in meeting the whole array of complex challenges? Is the pursuit of a specific functional security strategy, along with the adaption of deterrence as denial-of-benefit, the most effective and comprehensive policy option to manage network security? And would a cooperative security approach through international institutions be a viable alternative to complement self-help logics and to mitigate security externalities?

The paper thus aims to provide a policy-relevant analysis of the emerging cyber space security challenges facing the European Union, and the Transatlantic community more broadly, both in terms of threat’s strategic significance and of response options’ availability, and to subsequently identify the potential for the EU in exploring governance opportunities for “effective multilateralism” in cyber security affairs. After outlining the strategic character of the cyber threat and the constrained scope of self-help responses, an analysis of the opportunity for Europe to influence the current global securitization process of the cyber space (Sharma, 2010) is provided. The potential role of an EU cyber strategy to shape the undergoing strategic debate in Euro-Atlantic structures and foster global multilateral solutions and institutionalized cooperation (Gheciu, 2008), by promoting confidence building measures, is conceptualized through the broader theoretical assessment of the impact of multilateral institutions on emerging securitization processes (Buzan, Wæver, de Wilde, 1998), according to both rationalist and constructivist institutionalist perspectives (Keohane and Wallander, 1999).

An argument is therefore made for the unique institutional characteristics of the EU to represent - somehow counterintuitively - a strategic enabler for fostering an inclusive global cyber order, leveraged on the Union’s multilevel governance and transformative power capacity as a catalysts for cooperation (Lavenex and Schimmelfennig, 2009). The inherent limited effectiveness of competitive security postures in cyber space ultimately underscores the scope for pursuing cooperative approaches to avoid further militarization of the cyber dimension and a cyber arms race (Brimley, 2010; Geers, 2010). Contrary to the current declinist rhetoric, the EU has instead a robust comparative advantage to exercise its smart power in the cyber space to benignly shape such fundamental dimension of the global security architecture, through its negotiating capacity in the multilateral arena and its post modern de-securitizing capacity in the form of institutional density and normative strategic narrative.

The paper proceeds as follows. After outlining the theoretical perspective informing the paper’s analysis, the issue of the rising salience of the cyber strategic domain, its progressive securitization and the current state of policy responses are discussed. Subsequently, the paper provides a critical evaluation of the policy course centered on
the assumption of fairly unavoidable competitive scenarios. Finally, it formulates a proposal for an alternative policy option aimed at mitigating the unrestrained self-help logic by fostering a “cooperative” security approach, through international institutions and multilateral diplomacy. The paper concludes with a recommendation for the EU to take the lead in fostering strategic dialogue on cyber issue, in shaping the agenda of cyber security and in pursuing cooperative and inclusive strategies to ensure sustainable cyber security governance.
ANALYTICAL FRAMEWORK: SECURITY AND INSTITUTIONS

For the purpose of assessing the current state of policy responses to cyber threats and the availability of alternatives, the paper adopts a specific theoretical framework to inform the analysis of security relations, as well as the conceptualization of both competitive dynamics and potential prospects for cooperation and strategic stability in the cyber domain. Such analytical perspective combines the insights of constructivist security studies with the contribution of institutionalist theory, in order to depict both the essential character of security dynamics in the cyber domain and the prospects for mitigating such process through international institutions. The following paragraphs summarize the central tenets of both approaches and elaborate on how the integration of securitization and institutionalism can offer important insights into the emergence of institutionalized cooperative behavior in security affairs.

First, “security” is understood, for the scope of this paper, through the theoretical prisms of securitization theory (Buzan, Waever, and deWilde, 1998). Originated within the widening move in International Security Studies (Buzan and Hansen, 2009) with a distinctive constructivist orientation (Farell, 2002; McDonald, 2008), securitization theory has determined a shift of traditional strategic studies away from “objective” threat assessment to a wider, process-oriented conception of security, by focusing on how a securitizing actor transforms an issue into an existential threat by means of a “speech act”. The process of threat construction unfolds along a continuum stretching from normal politics to the realm of the “existentially threatening” requiring exceptional policy measures. In most cases the threatened object is the state (referent object), but it may also be identity, the environment, a political system or the economy, each time at a specific level of analysis (global, regional or sub-state). Finally, successfully securitized issues can be reversed into the dimension of normal politics, which is less conducive to violent conflict, and essentially de-securitized (Waever, 1995). The theory has the advantage of allowing the analyst to pinpoint security constellations in their material and social components, encompassing different typology of actors, threats (material and immaterial), and to appreciate the relationality and mutual social construction of the security dilemma (Booth and Wheeler, 2008). These characteristics make such a theoretical approach particularly adequate for exploring cyber threats, given the multi-layered nature of the domain (Libicki, 2009), the plurality of actors involved as sources or targets of threats and the inherent risk affecting the whole of human activity with extensive sectoral repercussions.

Secondly, as far as the theoretical literature on international institutions is concerned, both rationalist and constructivist institutionalism provide an appropriate analytical framework to examine the type of impact multilateral organizations and international cooperation can achieve on unfolding securitization processes and on the management of security relations (Keohane and Wallander, 1999). According to rational institutionalism, states are characterized by a consequentialist behavior determined by
material rewards and sanctions (Ruggie, 1998:855). International institutions affect such instrumental cost/benefit calculations by increasing transparency and by reducing information asymmetries, uncertainty and transaction costs. Functional knowledge, providing a focal point to solve cooperation problems, can also alter strategic calculations (Goldstein and Keohane, 1993:3-26). Constructivist institutionalism (Ruggie, 1998:869), instead, posits international organizations as social environments shaping actors’ compliance with ideational factors that re-define identities and preferences (Risse-Kappen, 1996), which are instead fixed under a rationalist perspective. States’ behavioral patterns follow a logic-of-appropriateness, which might ultimately lead to an internalization of norms (Johnston, 2001).

This paper advances a hypothesis for institutions to constitute an intervening variable affecting and mitigating the social construction of threats and the strategic behavior of states in responding to perceived threats. By combining securitization theory and institutionalism through a sequencing technique, it is possible to conceive the process of threat construction as unfolding in a relatively dense institutional environment, that not only shapes behavior according to a payoff matrix paradigm, but also re-constructs states’ identities in their mutual repeated interactions. Interstate cooperation’s production of functional knowledge through the action of epistemic communities (Adler, 2008) can lead in fact to the emergence of norms and values reconstructing states’ preferences through a logic-of-appropriateness. Subsequently, such complex cooperative learning process impacts retroactively on securitization and mitigates the process of definition of existential threats, not dissimilarly to what happens, albeit with greater magnitude, in the case of security communities (Adler, 2008). As far as cyber security is concerned, the paper’s argument for the policy option of exploring potential cooperative approaches, to complement current security policy responses, is consequently underpinned by the notion of international institutions’ capacity to structure, manage and mitigate securitization processes, thereby fostering strategic stability and moderating competitive dynamics.

1 Made possible by institutions’ reduction of uncertainty.
THE RISING STRATEGIC SALIENCE OF THE CYBER DOMAIN

The impressive development of information and communication technology, of computer networks, and of digital convergence certainly represents a dynamic that has distinctly characterized the economic and social progress of the last decades, linking the physical world of critical infrastructure with the virtual realm of the message and content being produced and transmitted (Castells, 2009). As cyber space has become an essential component underpinning civilian economic activity in virtually every sector, from finance to the media industry, it has also proved to be increasingly critical for government and military activities, diplomacy and public affairs (Potter, 2002). Therefore, similarly to past scientific innovations, an exogenous technological development is fostering a re-definition of military and defense policy, altering the strategic equation by affecting the evolution of the offense/defense balance, capabilities, and vulnerabilities (Nye, 2010).

The increasing salience of the cyber space as a strategic domain has progressively emerged along the interplay of two essential factors: a strong positive correlation between dependency and vulnerability, and a noticeable quantitative increase of cyber attacks - incentivized by the dependency factor - that has demonstrated the presence of a growing ability to exploit the inherent openness of the cyber domain to inflict significant damage.

First, the increasing pervasiveness, in both civilian and government spheres, of information and communication technology has underscored the issue of over-reliance on networks for a wide series of activity (from information security, to the operation of complex services), whose disruption can generate substantive damage (Brechbühl, Bruce, Dynes, and Johnson, 2010). However, it is the military sector, in particular, that has shown a significant dependence on a reliable and secure cyber space, given the preponderance of the net-centric warfare paradigm, generated by the technology-driven RMAs, which is heavily dependent on integrated C^4ISR to prevail in highly kinetic operational environments. Such over-reliability on the information technology for force projection and full-spectrum dominance has in fact incentivized less capable opponents to pursue asymmetric strategies in order to avoid confrontation at a high level of technology, while disrupt hostile technological assets (Sharma, 2010). The cyber domain can thus represent both a strategic enabler and a strategic equalizer, according to actors’ degree of technological dependency.

Secondly, a series of hostile events of growing complexity has occurred in cyber space, targeting services and infrastructures, from Estonia to Georgia, and lately to Iran. An exponential sophistication in attack codes’ architecture has emerged, underlining the attacker’s capacity to shift its focus from information disruption in the virtual domain - typically by achieving denial of service - to the neutralization of critical infrastructure, controlled and operated by networks in the physical world. As a consequence of both a steady awareness of such ICT dependency and of the clear sense of urgency in front of
hostile operations, the cyber domain has acquired an increasing strategic salience and to become part of the international security agenda.

Several governments have in fact started to explicitly include security in the cyber domain as an specific item in their most recent periodic defense reviews, to develop specific doctrines and to the establish military bureaucracies to meet cyber challenges. A clear securitization process of cyber space has been unfolding, with government officials performing a series securitizing moves that can be traced in strategic and planning documents, executive orders and public addresses. If states’ receptiveness to the salience of the cyber domain is at present indisputable, it is however less clear what has been identified as the referent object of such security utterances (Hansen and Nissembaum, 2010). In fact, the cyber domain’s property to blur real and virtual, civilian and military, threat and objective has been mirrored in the difficulty to discretely define what should be defended by whom. Moreover, given the wide spectrum of damage that a cyber attack can inflict, the urgency of the threat varies across the sectors, from a maximum degree in the disruption of military systems of command and control, to an intermediate one in the case of collapse of critical infrastructure, to a relatively modest one as far as economic activity is concerned (Cornish, Hughes, and Livingstone, 2009).

In conclusion, it can be argued that a clear securitizing move has invested the military sector and has identified in the government network the object of protection and in the adaptation of classical concepts of deterrence, offense and defense the aim of security policy. However, such process has not extended, at least formally, to the economic, societal and political domains. The potential militarization of the cyber domain or a hyper-securitization of the whole of the cyber activities has been avoided, partially as a result of the inherent structure of information networks, as well as a conscious decision to discriminate and limit the process of casting of cyber in terms of “existentially threatening”.

THE CYBER DOMAIN AND EMERGING SECURITY POLICY

The increasingly salient role of the “fifth domain” in the XXI century security environment, underpinned by a growing awareness of dependency, vulnerability and sense of urgency in light of cyberkinetic events, has led to the formulation of reactive policy responses. National governments and international organizations alike have started to establish ad-hoc bureaucracies and to define their mission, lines of authority, and functional responsibilities. In this respect, the US has taken the lead, within the Transatlantic community, in creating a dedicated CYBERCOM, while European nations have created offices of coordination and NATO an Allied center of excellence for cyber security.

However, the very nature of the strategic domain, and its relations to the broader security environment, represents the most daunting obstacle for policy formulation. The literature has extensively outlined the complex dimensions of cyber space, depicting it as a unique man-made and technology-driven strategic domain. It is structured according to a network model, with a noticeable degree of openness and high speed of transmission, which complicates control. Cyber space could thus be defined as the fundamental infrastructure of advanced modernity, combining cognitive and material dimensions and interconnecting nodes according to a non-hierarchical logic that transcends Westphalian notion of territoriality, boundaries, monopoly and sovereignty. Moreover, technological specifications enable identities to be concealed, along with sources of information and potential threats (Lynn, 2010), thereby contributing to the inherent state of uncertainty and systemic risk. Finally, as already pointed out, cyber space presents the co-presence of several actors with substantially different agendas, from a criminal to a terrorist, from an economic to a political one. Accordingly, cyber threats can be understood along a spectrum integrating the degree of inflicted damage with the typology of perpetrator (Cornish, Hughes, and Livingstone, 2009). Such characteristic ultimately underscore the fact that cyber space can simultaneously be a vehicle of threats to both the physical and the information world and towards other domains integrated in a strategic unicum.

As previously noted, despite cyber space’s relevance not only for the military, but also for the economic, political and societal domains, the securitizing move and the subsequent policy responses have so far concentrated exclusively on the protection of militarily essential network and critical infrastructure. However, the very integrated architecture of networks makes it increasingly difficult for security policy to discriminate between vital and non-vital systems, and civilian and military factors. In addition to this preliminary definition of the scope in cyber protection, security policy has identified three layers of cyber space, namely the “physical, syntactic and semantic” (Libicki, 2009) - respectively hardware, software and content – to be the core objectives of its action.

Firstly, emerging cyber security policy has thus centered on the concepts of functional security, aiming at increasing resilience of critical infrastructure, and of civic security focused on societal response to disasters. Given the structural asymmetry between relatively inexpensive capabilities required for launching an attack and a costly, inefficient
and rapidly obsolete defense, cyber security policy has focused on minimizing the impact of hostile events and denying their expected outcomes. Such strategy remarkably captures the essence of cyber power as “the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain” (Nye, 2010:3-4).

Secondly, policy-makers had to endeavor to re-define the notion of deterrence. Because of the impracticability of retaliatory action (constrained by the technically-limited traceability of attackers) the focus of security policy has shifted toward the adaptation of deterrence as denial-of-benefit, which aims at increasing the network’s resilience, in both its logical and physical components (Lynn, 2010). Deterrence in cyber space cannot adopt a countervalue posture, for the enduring principle of a denial-of-attribution plausibility, due to the dispersed and diffused character of threats. The attack is therefore not countered per se, but by strengthening the defendant’s network resiliency, thereby negating the attended objective of the attacker.

Finally, in order to overcome the conflation of defense and deterrence, an attempt is being undertaken to conceive further options to complement deterrence as denial-of-benefit and defense as vulnerability minimization, with challenges of cyber warfare (Libicki, 2009). The development of offensive capabilities has thus been contemplated - as the final side of the cyber strategic triad - in order to enable the performance of both retaliatory operation and signaling activity for escalation dominance (Goodman, 2010), despite the persistence of attributional uncertainty and of a limited capacity to discriminate military objectives.
CHALLENGES TO CURRENT STRATEGIC POLICY

The progressive formulation of a cyber security policy focused on *functional resilience* and *denial-of-benefit*, despite capturing the profound implication of the new domain, presents nevertheless a series of problematic aspects. The underlining challenges to current strategic policy can be understood along three key interrelated categories: *attribution*, *discrimination*, and *dispersion*.

First, the issue of *denial-of-attribution plausibility* dramatically restrains the scope of deterrence policy, in a context of already depleted defense options, given both the positive correlation between cyber dependency and vulnerability and the asymmetries between offense and defense in terms of required capabilities. As previously noted, at the present state of technology, attack codes can be designed to avoid traceability: a typical case is represented by “bot.net”’s capacity to hijack systems that become part of a complex attack sequence. Consequently, the solution of pursuing *denial-of-benefit through resilience* as a form of deterrence constitutes a reasonable but necessarily limited solution to counter the threat. Furthermore, the potential development of offensive capabilities, and of a countervalue posture, to achieve mutual deterrence is hugely controversial, because the uncertainty in attribution would translate in greater instability (Harknett, Callaghany, Kauffman, 2010).

Second, intertwined with traceability, the question of *discrimination* is equally of critical importance in the cyber domain for both the legal and strategic decision-making spheres (Shackelford, 2009). In addition to the difficulties in defining what precisely constitutes a cyber attack, humanitarian law and the law of armed conflict are challenged by an increasing problematic distinction between military and non-military aspects, civilians and belligerents (Huges, 2010). This aspect, moreover, is also of fundamental importance for *strategic brinkmanship* calculations - that rests upon the shared perception of force thresholds - and for avoiding a *functional security overstretch*, that may be forced to be applied to the whole of national networks because of discrimination issues. Therefore, discrimination constitutes an additional limitation to the operationalization of resilience strategy and to the achievement of an eventual equilibrium centered on mutual deterrence-by-punishment.

Finally, threat and vulnerability *dispersion*, by linking the issues of *attribution* and *discrimination* and their implications on defense, deterrence and strategic calculations, represents an overarching challenge to cyber security policy’s *coherence* and *effectiveness*. In fact, the emphasis on the improvement of networks’ resilience across the three relevant layers of cyber space, in a context of inherently blurred boundaries between civilian and military spheres and between the sources of threats, suggests a potential indefinite extension of the scope of security policy. The more comprehensive functional resilience policy becomes, however, the higher the incentives for attackers to expand their target sets. Over-stretch of functional security in cyber space would consequently have significant negative repercussions in terms of its effectiveness, but
also of its overall purpose, as it would be paradoxically conducive a deterioration of the competitive logic of security relations in cyber space, by igniting an *hyper-securitization* process (Hansen and Nissembaum, 2010).

In conclusion, the overall policy rationale proves to be unsatisfactorily constrained between, on one hand, a de-stabilizing *hyper-securitization* and *weaponization* of cyberspace, and the limited scope of action for *protection and denial-of-benefit*, on the other.
**ALTERNATIVE POLICY OPTIONS: COOPERATIVE SECURITY AND CONFIDENCE BUILDING**

The analysis of the challenges facing cyber security policy based on a functional security model has identified a series of weaknesses, in terms of *effectiveness*, *efficiency* and *sustainability*, which provide the scope for seeking to formulate an alternative and complementary approach. In fact, respectively declined in terms of resilience and denial-of-benefit, defense and deterrence’s overlapping functions provide a realistic, yet inevitably partial, response to meet cyber challenges. Equally, cyber space’s nodal and multi-layered architecture, by conflating the notion of embedded *risks* and induced *threats*, underscores the need to conceive responses that fully consider the issue of *security relationality* and the role of *inclusive governance*. Ultimately, the specific role of deterrence in the cyber domain - along with the risk of overstretch of functional security under the capability/vulnerability asymmetry - adversely affects the *dependability* of self-help measures, underpinned by an *oppositional* perspective on security.

Therefore, a higher degree of policy effectiveness can instead be achieved through the pursuit of a strategy aimed at influencing the *relational* development of security dynamics in cyber space. Such policy approach would shift the focus from cyber capabilities, vulnerabilities and damage control postures, to the implementation of a *cooperative engagement* through an increased *institution-based* multi-stakeholders’ *strategic dialogue* and *comprehensive negotiation* track. The overall purpose of such course would be to offer a complementary instrument to current security policy. By exploring *governance* options to restrict externalities, such as cyber crime, and to *build confidence* among relevant actors, in order to increase transparency and reduce uncertainties, cooperative confidence building can yield an impact on the *threat construction* process and fill the shortcomings of self-help logics.

For this purpose, *security management institutions* (Keohane and Wallander, 1999) constitute a most adequate typology of institution capable of channeling cooperative engagement and to exert a meaningful role for multilateral cyber security affairs. Their rationale in fact allows for a comprehensive, inclusive and cooperative management of common threat and risks, by fostering strategic dialogue on doctrines and postures while providing the necessary level of transparency and predictability that creates confidence among the membership and ultimately security.

As systemic risk is *inherent*, threats originate from different sources, and attribution opacity curtails the stabilizing role of deterrence, the cyber domain’s security externalities are broadly compatible with the logic of security management institutions. First, their criterion of *inclusive multilateral participation* is required by cyber threats’ pervasiveness.

---

2 The OSCE and NATO with its PIP/EAPC and “global connectivity” partnership arrangements constitute examples of organizations that operate according to a principle of inclusive and cooperative management of common threat or risks, with a relatively strong degree of legalization.
affecting states, but also other vulnerable stakeholders. Secondly, their capacity to address emerging *common risks* cooperatively and continuatively, by providing their membership with functional knowledge, transparency and predictability, is highly relevant for cyber affairs. The cyber domain, as discussed, presents diffused, *poorly traceable threats* that are blurred with the inherent *risks* proper of network’s physical and logic architecture, which represents a shared global concern.

Institutions would thus allow for a shared production of information, the emergence of transnational epistemic communities’ expert knowledge, and the establishment of cyber *confidence building measures*, subject to technical feasibility under the current internet governance architecture. Stakeholders’ *strategic expectations* would be shaped and *norms* would progressively emerge, firstly as *regulative principles* for simple utility-driven cooperation and secondly as *deeper social values* with a potential for affecting perception and *mutual social construction of threats* (Waever, 1995).

As underlined in the literature, the legal challenges for negotiation of a cyber convention to regulate states’ and other actors’ behavior, including the issue of control of offensive actions and limitation of capabilities development, are significant both in terms of actual definition and scope for agreement, but also in terms of actual applicability and compliance (Hughes, 2010). Therefore, cooperation should focus preliminary on developing a common understanding of security challenges through multilateral engagement and subsequently on the production of legally binding rules and on the issue of compliance. More than premature a legally binding treaty regulating the development, transmission and use of attack codes (Brimley, 2010), or improving internet governance, it is paramount to foster strategic dialogue, develop *common knowledge* on cyber warfare *doctrine* and *operational postures*, to foster the interaction between epistemic communities, and in so doing, above all, build confidence.

In this respect, the EU is in a unique position to exert a fundamental role in shaping the agenda of global cyber affairs and to foster such cooperative track through relevant existing institutional frameworks for multilateral diplomacy. The EU’s *external governance projection* (Lavenex, Schimmelfennig, 2009), strongly rooted on a *rule-based* model and on global engagement, enables to foster international dialogue on cyber issues, for four main reasons. First, its technological capacity makes it a critical player, both in terms of global share of civilian *industrial and research capacity*, and in terms of potential development of capabilities of military significance. Secondly, its perception as a civilian power, or at least as a security actor characterized by a specific focus on *effective multilateralism* and international order, allows the EU to act vis-à-vis emerging powers as a genuine global broker devoid of a primacist agenda (Cornish, Edwards, 2005). Thirdly, because of its universal *functional scope* and *institutional capacity* (JHA, ESDP, Community pillar) to consider simultaneously several aspects of cyber affairs, from the

---

3 Non-state cyber stakeholder, often possessing a remarkable degree of capacity, could be involved along a
criminal to the strategic dimension, the EU can make a very extensive contribution in terms of regulation, expertise and *multi-stakeholder governance*. Fourthly, because it has the potential to aggregate European States’ national efforts, the EU can create a critical mass to shape the agenda at the global level, while representing a meaningful partner at the transatlantic level, a coherent actor in regional *fora* and at the global multilateral level.
CONCLUSION AND POLICY RECOMMENDATIONS: MANAGING CYBER INSECURITY

The paper’s analysis of the emerging security policy and of its key challenges has raised a series of points with implications for both the theoretical and the policy debate.

At the theoretical level, cyber space provides an example of how international institutions have an opportunity to mediate, mitigate, and even shape a securitization process and the emergence of security patterns. By combining securitization and institutional theory, the analysis of the state of play of cyber security policy allows to appreciate an alternative policy course, based on cooperative engagement that proves to be realistic given the shortcoming of self-help options. Institutions as social environments can represent an intervening structural variable to the securitization process unfolding within the membership, by shaping expectations and altering both rational calculations, and the social construction of threats.

At the policy level, the policy course proposed constitutes a reasonable alternative to the intertwined problematic full-scale cyber space weaponization and insufficient functional security approach. Cyber space’s technical characteristics qualify threats and vulnerabilities in such a way that makes security policy options based on self-help unsatisfactory. An incentive for seeking cooperative security solutions based on institutionalized security dialogue and confidence building, as instruments to mitigate and manage competitive dynamics and avoid cyber chaos, is thus to be found in the shortcomings of the however necessary resilience options. The relevancy of such course lies in institutions’ role in providing a platform for epistemic communities to develop both functional and principled knowledge that could help to structure cyber strategic relations and foster stability, similarly to conventional and nuclear domains in the past.

In conclusion, three policy recommendations for the EU emerge from the analysis conducted:

The EU should engage more decidedly in cyber affairs and acquire more integrated responsibilities to avoid redundancies with national polices and leverage its broad institutional capacity to review European cyber security status, identify and monitor vulnerabilities and streamline necessary actions, backed with credible financial support.

A cyber coordination cell at the Secretariat of the Council would be a welcomed institutional development as a first step to insert cyber strategic affairs on the EU agenda. Cyber security should find an appropriate place in the European security documents.

The EU should take the lead in multilateral affairs on cyber security and engage capable states at the regional and global level, with the aim to mitigate competitive trends by devising confidence building measure and ultimately explore potential for treaty negotiation.
In today’s complex interdependent global security environment, as a *sui generis* actor simultaneously representing an unprecedented post-modern evolution of international politics (Cooper, 2003), the EU has the unique possibility of experimenting an equally innovative approach to cyber security affairs. The emergence of a cyber agenda represents a fundamental opportunity for Europe to take the lead in exploring an alternative policy track, by focusing on the missing cyber strategy aspect of institutionally-facilitated stabilization of expectations, reduction of uncertainty, and management of inherent systemic risk.
BIBLIOGRAPHY


Clark, I. Legitimacy in international society, Oxford, Oxford University Press, 2005


European Union High Representative for CFSP “A secure Europe in a better world: European Security Strategy”, Brussels, 12 December 2003


Libicki, M. *Cyberdeterrence and Cyberwar*, Santa Monica, RAND, 2009


**Multilateral and national reports on cybersecurity**


