The EU and NATO: Cyber-Security Partners or Divergent Actors? An Exercise in Framework Development

Tarun Chaudhary
Ph.D. Candidate
International Affairs, Science and Technology

Sam Nunn School of International Affairs
Georgia Institute of Technology
Atlanta, GA

gte293y@mail.gatech.edu
+1 (678)-524-5466

Prepared for the European Union Studies Association Conference

March 2015
Boston, MA

Please Do Not Cite or Distribute This document is a DRAFT

Abstract: *With the continually evolving importance of cyber strategy in European affairs, multi-stakeholder organizations such the EU and NATO are struggling to articulate cyber-security initiatives to address a wide variety of needs and imperatives. This paper will assemble a framework with which to critically analyze and explore the emerging NATO and EU cyber-security dynamic by building bridges between regime complex theory and the Choucri & Clark layered model of cyber-space. In addition the argument will be made to shift away from the term 'cyber-security' and instead focus on 'information-security management' at various levels of abstraction and analysis. It is proposed the emerging EU/NATO dynamic can be understood within the detailed framework where 'chessboard politics' inherent to regime complexes can be focused upon through usage of a layered model of cyber-space.*

It is patently obvious that *cyberspace* has become a strategic security concept in and of itself. Whether viewed as a constituent battlespace, a technological infrastructure, a socio-cultural concept, or an economic engine – information exchanged, stored and processed via electronic means and accessible through a variety of vectors to an international user-base has, for better or worse, become a central security concern for governments. It is unsurprising then, that governments would seek to create bureaucratic infrastructure around and for cyber-security. NATO has, since 2008, acknowledged cyber-security as one of their foremost areas of interest and the organization maintains amongst other offices, a "Cyber Defence Centre of Excellence (CCDCOE)" in Estonia. The EU has published a Cybersecurity Strategy that emphasizes the creation of EU wide cyber-defense policy within the framework of the larger European Common Security and Defense Policy (CSDP) pillar of EU integration and collaboration. In addition, the European Union Agency for Network and Information Security (ENISA) acts as the central broker of information security related policy guidance within the EU. This is on top of the emphasis on cyber-security put forward by individual EU member states along with their own strategies and attendant bureaucratic/institutional structures. Given the complementary nature of NATO/ CSDP security mandates, it is somewhat surprising that very little work, academic or policy oriented, exists to spell out the converging or diverging natures of cyber-security strategy, policy, and implementation between the two bureaucratic entities. This could be the case for a variety of reasons, amongst which are the vexing ambiguity and imprecision of the term "cyber-security", the difficulty in segmenting and assessing the variety of formal and informal

institutions involved in 'cyber-security' and cyber-governance which fall across civil/military and public/private lines, and few frameworks available, if any, on which to base analysis that are able to successfully conceptualize the information space alongside the trans-national political space (of which have also been widely accepted or applied).

This paper is meant to serve as an organizing tool and first cut at finding a way out of the morass in order to better understand the evolving relationship between the NATO and the EU with regards to the cyber-security. While that specific subject is understudied, there is ample work that looks at the overlapping nature of NATO and CSDP concerns generally, along with a burgeoning literature on regime complexes. Regime complexes are defined by loose affiliation amongst regimes within an issue-specific area of focus, in this case cyber-security.[1] Several guiding assumptions will be made before proceeding. 1) The definitional ambiguity of the term '*cyber*-security', while well worth discussing, cannot be solved here and will vary given institutional and regime context. 2) The overlapping, nested, and the otherwise complex relationship amongst cyber related institutions, regimes, bureaucracies, and normative milieu is larger than what can easily be mapped directly. 3) Existing frameworks related to security studies and international regimes can be harnessed to effectively explore and understand intergovernmental cyber-security relationships, though empirical observation of ongoing and future dynamics may be difficult. To that end, this paper is concerned with articulating a frame-work to examine the NATO/EU (perhaps more specifically CSDP) cyber security space by building bridges between regime complex theory as articulated by Hofmann, Nye, and others and Choucri and Clark's layered model of cyber-space. for assessing and understanding international context with regards to the Internet. In addition, the attempt will be made to relax reliance on the term 'cyber-security' and instead shift toward an analysis of *information-security management*, drawing on computational and information sciences definitions of the term, at various levels of abstraction and analysis.

This paper will proceed in three sections; the first will introduce the idea of "information security management" and argue it should be substituted for the term 'cyber-security'. The second section will build connections between disparate treatments of regime complex theory to integrate the discussion of EU/NATO security overlap with cyber-security. The third section will propose the usage Choucri and Clark's layered model of cyber-space to systematically analyze facets EU/NATO cyber-security dynamics across several levels of analysis.

Shifting Away from *Cyber*

Cyber-security as a term lacks a coherent or singular meaning. This is an often-made observation within the burgeoning cyber focused literature emanating from the collective disciplines falling loosely under the rubric of international studies. Writers usually follow the observation by a parsing of the term before a definition is offered that tries to bring clarity within the context of an author's purpose. While the present work is no different, the argument will be made here that this definitional ambiguity cannot be solved due to a variety of normative and conceptual linkages the term gains when used within specific institutional context or in an area

[1] Nye, Joseph S. "The Regime Complex for Managing Global Cyber Activities." (2014). Available at: http://dash.harvard.edu/handle/1/12308565

specific manner. In order to sidestep the debate over what 'cyber-security' means, a substitution can be made to analyze "information security management" at various levels of analysis and abstraction. The latter term being drawn from the computational and information technology disciplines and defined using the well-established McCumber Cube model of information security management. The model is often taught to students of information technology and computing as a way to frame security along multiple dimensions of organizational foci. Information is conceived as being in one of three stages: storage, processing, or transmission. Each of these three stages is given an axis in the model's representation. In addition, information can be compromised in (any combination of) three ways defined by, confidentiality, integrity, and availability.[2] The US National Institute of Standards and Technology (NIST) gives the following definitions of objectives for each dimension:

- *Confidentiality* –"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information"
- *Integrity* – "Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity."
- *Availability* – "Ensuring timely and reliable access to and use of information."[3]

The combined six dimensions can be represented as such:

	Storage	Processing	Transmission
Confidentiality			
Integrity			
Availability			

Figure 1: Simplified Model of Information Security

Within this conception, security is envisioned as being managed in a holistic way that pays attention to each intersecting state of information through each possible vector of compromise. The traditional McCumber Cube adds another three dimensions turning the above two-

[2] Over the past two decades, this model has been firmly ensconced within computing security, however for a general overview of the model see: Maconachy, W. Victor, et al. "A model for information assurance: An integrated approach." *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*. Vol. 310. New York, USA, 2001.

[3] NIST FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems available at: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

dimensional grid into a three-dimensional shape, however for the purposes of this discussion, the simplified model shown above will suffice. Using this as a heuristic, the definitional quandary resulting from the ill-defined term 'cyber-security' can be avoided by focusing on the constituent make-up of all things 'cyber', which is of course: information. Security is thereby incumbent upon maintaining the confidentiality, integrity, and availability of information as it is being stored, transmitted and processed. This does not change weather a computer scientist, CTO, political scientist, or layperson is discussing a 'cyber' prefixed topic. It also does not change as discussion moves away from computing hardware to ever more abstract levels incorporating political, cultural, and social dynamics. In the end, 'security' comes down to assuring the six dimensions above are addressed for information at all levels of analysis, from individuals to the systemic level of nations-states and the various electronic networks intertwined therein.

Admittedly, the argument for this substitution and idiomatic shift in terminology is not robustly developed here, however the following pages will attempt to lay bare the logic and utility doing so through application of the above model of security through several levels of analysis and abstraction. Having established a basis to understand information security management, the next section will introduce regime complex theory as a way to analyze evolving information governance and security institutions and norms.

NATO and EU Security Overlap

The policy and institutional locus between NATO and European Common Security and Defense Policy (CSDP) has been analyzed with some vigor. Scholars, just as Hofmann and others have used a variety of methods to discuss evolving patterns of institutionalism, governance and power relations that describe how each institution has contributed to the fabric of European security policy and identity. Indeed there is a large amount of overlap between the two institutions in terms of membership, and formal agreements exist linking NATO to the EU security agenda both in spirit and function (and vice versa).[4] Analytic schools and traditions have evolved around conceptual centers of gravity, which include institutional, governance, power-based and regime based frame-works.[5] The route pursued here is to follow Hofmann and others whom have described the EU/NATO relationship as representing a 'complex regime'. Regimes are a formalized set of norms and regime complexes are the loose affiliation amongst regimes that lay between formal legal instruments and disparate patchworks of applicable regimes with regard to an issue area.[6] Regime complexes are identified by the existence of overlap between institutions, and Hofmann identifies three dimensions of overlap: membership, mandate, and resources. She identifies the 21 members which overlap both NATO membership and common European defense policy and discusses the idea both organizations have mandates centered on crisis management. In terms of resources, the 2003 Berlin Plus agreement gives the EU access to NATO assets including the following:

[4] "Overlapping Institutions In The Realm Of International Security: The Case Of NATO And ESDP." (2009): *OAIster*. Web. 27 Feb. 2015.
[5] Regime complexity is a growing pool of literature; see for example Keohane, Robert O., and David G. Victor. "The regime complex for climate change." *Perspectives on politics* 9.01 (2011): 7-23.; Orsini, Amandine, Jean-Frédéric Morin, and Oran Young. "Regime complexes: A buzz, a boom, or a boost for global governance?." *Global Governance: A Review of Multilateralism and International Organizations* 19.1 (2013): 27-39.; Karen J. Alter and Sophie Meunier (2009). The Politics of International Regime Complexity. Perspectives on Politics, 7, pp 13-24.
[6] Nye 2014, p.5

- "A NATO-EU Security Agreement that covers the exchange of classified information under reciprocal security protection rules;
- "Assured access to NATO planning capabilities for EU-led operations;
- "Availability of NATO assets and capabilities for EU-led civil-military operations;
- "Procedures for release, monitoring, return and recall of NATO assets and capabilities;
- "Terms of reference for using NATO's DSACEUR (Deputy Supreme Allied Commander Europe) for commanding EU-led operations;
- "EU-NATO consultation arrangements in the context of an EU-led operations making use of NATO assets and capabilities;
- "Arrangements for coherent and mutually reinforcing capability requirements, in particular the incorporation within NATO's defence planning of the military needs and capabilities that may be required for EU-led military operations."[7]

Hofmann uses the Berlin Plus agreement as a narrative device to discuss a typology of behaviors inherent to the regime complexity, referred to by her and others commonly as "chessboard politics".[8] The term describes the manner in which institutional overlap leads to strategies resulting in both intentional and unintentional effects, which originate in internal dynamics that then have consequences within the other overlapping/opposing institution. The practice is akin to one side in a chess match moving their own pieces that then force a re-arrangement of the opposing side's pawns, knights, bishops, king and queen. Hofmann states such "chessboard politics" manifest themselves in member state strategies that she calls "'hostage taking,' 'turf battles,' and 'muddling through.'"[9] Using the example of Cyprus and Turkey, Hofmann shows how each country was able to take advantage of their position to shape the relationship between their two respective organizations (the EU and NATO) despite neither being reciprocal members of both organizations, this 'hostage' taking relies on overlapping regime connectivity and not on direct control of consequences. The 'turf-battle' strategy is used to differentiate, shape and influence mandates of involved organizations to include or exclude various interests. Hofmann cites the view taken by Belgium, Luxembourg, and Spain during the Berlin Plus negotiations that favored ESDP (now called CDSP) as an autonomous alternative to NATO instead of the closer arrangement detailed above. When the two strategies are implemented, it can lead to the situation where a clear division of labor between institutions does not develop and the resulting dynamic is one in which ambiguity reigns and informal alternatives are sought –the act of muddling through as it were. Hofmann's assessment is useful as it lends a several 'sign posts' to look for when analyzing systems displaying regime complexity, and better yet the template is tailored to the existing EU/ NATO security dynamic.

Cyber-space too has been described as representing a space governed through a myriad overlapping institutions, regimes, and norms. Most recently Joseph Nye has described the "Regime Complex for Managing Global Cyber Activities" within which there exists of subset across a large swath of the totality that impact upon security. Nye positions his work as a mapping exercise meant to describe the system as a whole, but readily admits a comprehensive direct mapping is not possible given the breadth of total involved entities, formal and informal, is vast. Thereby, it is useful to turn back toward the sign-posts provided by Hofmann to help zero

[7] About CSDP – The Berlin Plus Agreement, European Union External Action Service available at: http://eeas.europa.eu/csdp/about-csdp/berlin/index_en.htm
[8] Alter and Meunier 2009
[9] Hofmann 2009, p. 46

in on critical intersections of overlap between NATO and the EU to help better understand their evolving cyber-security dynamic. The membership overlap identified by Hofmann remains pertinent to the information security context, however in terms of mandate overlap there appears to be separation between the two institutions. Sliwinski submits NATO's conception of cyber-security is much narrower than the EU's and subsequently the CDSP. He characterizes the EU as "lacking a collective vision on cyber-security" citing that only 15 EU member states have national cyber-security strategies and the remaining 12 address cyber-security through their respective national security strategies.[10] NATO on the other hand, according to Sliwinski, has incorporated cyber-security into the most basic of its mandates. Indeed at the Wales Summit in 2014, NATO officially recognized 'cyber-attack' against a member-state as possibly triggering an Article V collective defense response. Threshold levels of 'damage' were not, however, specified (nor would they be expected to define such). Crime, while at the center of the EU information security context is less an area of focus for NATO, who's information security mandate is more traditional defense security oriented including defense information espionage and electronic networks as a vector of state on state conflict. In terms of resources, the overlap between the two remains defined by the Berlin Plus agreement, important parts of which regarding information security are classified. In order to proceed analysis should focus on areas in the EU/ NATO cyber-security relationship that display the types of behavior detailed by Hofmann. Namely where do we see hostage-taking, turf-battles, and muddling through in terms between the two entities with regard to cyberspace? Before such dynamics can be identified the evolving framework requires one more analytic tool before being applied. The next section will introduce Choucri and Clark's layered model of cyber-space.

Layered Model of Cyberspace

Choucri and Clark build upon the traditional layered model of the Internet in order to establish a typology of analysis that integrates, according to them, traditional international relations levels of analysis with the 'cyberspace'. Specifically, they're concerned with identifying a method of analysis that can used to understand "cyber-actors" in terms of power relations across specific points of control that vary between conceptual layers. Each layer relies additively on those appearing below to function. At the lowest level is the physical infrastructure upon which cyber-space functions such as optical fiber and other hardware. Above that sits the 'logical' layer, itself made up of three sections, the Internet, Services, and Applications. The TCP/IP packet protocol, for example, is part the 'Internet'. The Domain Name Service which translates numeric addresses into the Uniform Resource Identifier (URL) commonly associated with specific internet addresses which end in '.com', '.org' etc. is the middle of the logical layer. The application layer consists of what we commonly conceive up as the 'web' or the graphical and searchable portion of the Internet. The model then incorporates two top layers. The first is labeled, quite simply, 'information' and represents, "encoded text, photos, videos, and other material that is stored, transmitted, and transformed in cyberspace,"[11] At the very top, 'people'

[10] Sliwinski, Krzysztof Feliks. "Moving Beyond The European Union's Weakness As A Cyber-Security Agent."*Contemporary Security Policy* 35.3 (2014): 468-486. *Business Source Complete*. Web. 27 Feb.
[11] Choucri, Nazli, and David D. Clark. "Integrating cyberspace and international relations: The co-evolution dilemma." (2012) available at: http://ecir.mit.edu/images/stories/Clark_WORKSHOP.pdf

represent users and constituencies "who shape the cyber-experience and the nature of cyberspace itself"[12] Choucri and Clark present the following graphical representation of their model:

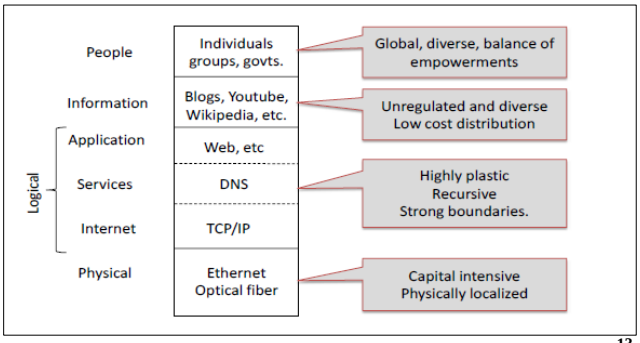

Figure 2: Choucri and Clark Layered Model of Cyberspace[13]

Traditional levels of global political analysis include the individual, state, and systemic (international system of states). Choucri and Clark introduce the following dimensions: Global which is non-state centered but global in nature (such as the issue of spam), Non-profit and Profit-seeking. The layers discussed above can be analyzed across the various levels of analysis. Their "Integrated Cyber-IR System" appears below, the 'logical layer' appears in dark grey. Examples of issues and actors are slotted into the matrix for illustrative purposes some of which appear in Choucri and Clark's similar graphic. Not all spaces are filled. The idea is to use the matrix to understand a particular issue or cyber-actor as a function of where they sit within the layers of cyber-space and the levels of analysis.

	Individual	**State**	**International**	**Global**	**Non-profits**	**Profit-seeking**
People		Military Use	NATO/ EU			
Information		Censorship		Spam		Information Control
Applications					W3C	
Services					ICANN	
Internet					IETF	
Physical	Home Wiring		Telecommunications regime	Satellite Orbits and Spectrum		Infrastructure companies (L3, Verizon, etc.)

Figure 3: Chourcri and Clark Integrated Cyber-IR System[14]

The additional nuance that can now be added to their 'integrated' system is the earlier described notion of information security management. Instead of trying to define 'cyber-security' across all the various and interactive layers and levels, 'information security management' can be thought of as having implications at each level. At each of the intersecting (and through combinations of) dimensions, information's confidentiality, integrity, and availability can be compromised as it is being stored transmitted and processed. The framework can now be used to map various facets of

[12] Ibid.
[13] Choucri and Clark 2012, p. 3
[14] Recreated and adapted from Choucri and Clark 2012

the NATO/EU cyber-security regime along with the larger cyber-governance regime detailed by Nye. This is not accomplished within the scope of the present paper which is meant to simply articulate the framework. However, initial forays into the exploration of the EU/NATO relationship seem to indicate, the EU is better positioned to propagate change within the cyber regime utilizing 'chessboard politics' than NATO despite the latter organizations more mature strategic cyber-security vision.

This initial framework was assembled in order to explore the burgeoning cyber-security relationship between the EU (and specifically the CDSP) and NATO. The argument was made that the term cyber-security is problematic and a substitution of terminology that focuses on information security management should be used to conceive of 'security' within this space which helps center discussion on the security of 'information' itself. The EU and NATO were detailed as representing a complex security regime, which following work by Hofmann and others, is said to display a specific typology of political behaviors termed, 'hostage-taking,' 'turf-battles,' and 'muddling through.' The paper concluded that in order to focus specifically on these behaviors within the 'cyber-security' regime complex, the Choucri and Clark layered model of cyber-space could be adapted. Next steps in this research process will map specific NATO/EU cyber-security concerned institutions onto the "Integrated Cyber-IR System" in order to analyze the nexus between such entities along with their connection to the larger 'cyber-governance' regime complex as detailed by Nye.

Sources

About CSDP – The Berlin Plus Agreement, European Union External Action Service available at: http://eeas.europa.eu/csdp/about-csdp/berlin/index_en.htm

Alter, Karen J., and Sophie Meunier. "The Politics of International Regime Complexity." *Perspectives on Politics* 2009: 13. JSTOR Journals. Web. 1 Mar. 2015.

Choucri, Nazli, and David D. Clark. "Integrating cyberspace and international relations: The co-evolution dilemma." (2012). Available at: http://ecir.mit.edu/images/stories/Clark_WORKSHOP.pdf

Choucri, Nazli. *Cyberpolitics In International Relations.*Cambridge, Mass. : MIT Press, (2012). Print.

Hofmann, Stephanie C. "Why Institutional Overlap Matters: CSDP In The European Security Architecture." Journal Of Common Market Studies 49.1 (2011): 101-120. Business Source Complete. Web. 4 Mar. 2015.

Hofmann, Stephanie C. "Overlapping Institutions In The Realm Of International Security: The Case Of NATO And ESDP." (2009): *OAIster*. Web. 27 Feb. 2015.

Keohane, Robert O., and David G. Victor. "The regime complex for climate change." *Perspectives on politics* 9.01 (2011): 7-23.;

Maconachy, W. Victor, et al. "A model for information assurance: An integrated approach." *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*. Vol. 310. New York, USA, 2001.

Merand, Frederic, Stephanie C. Hofmann, and Bastien Irondelle. "Governance And State Power: A Network Analysis Of European Security." *Journal Of Common Market Studies* 49.1 (2011): 121-147. EconLit. Web. 1 Mar. 2015.

NIST FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems available at: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Nye, Joseph S. "The Regime Complex for Managing Global Cyber Activities." (2014). Available at: http://dash.harvard.edu/handle/1/12308565

Orsini, Amandine, Jean-Frédéric Morin, and Oran Young. "Regime complexes: A buzz, a boom, or a boost for global governance?." *Global Governance: A Review of Multilateralism and International Organizations* 19.1 (2013): 27-39.

Sliwinski, Krzysztof Feliks. "Moving Beyond The European Union's Weakness As A Cyber-Security Agent." *Contemporary Security Policy* 35.3 (2014): 468-486. Business Source Complete. Web. 27 Feb. 2015.