An interview with Dr. Chris Demchak (Professor, Strategic Res. Dept; CoDir, Ctr Cyber Conflict Studies (C3S), United States Naval War College)

by Daniel Ventre[1] (*CNRS; Chair in Cyberdefense and Cybersecurity*)

May 2013 – Article n°III.3

Dr. Chris C. Demchak has a PhD from Berkeley (political science) with a focus on organization theory and complex systems, security studies, and surprise in largescale socio-technical systems across nations. She also holds two masters degrees, respectively, in economic development (Princeton) and energy engineering (Berkeley). She has published numerous articles on societal security difficulties with largescale information systems to include cyberwar and cyber privacy ("theory of action", "BIK behavior-based privacy"), security institutions (CT "Knowledge Nexus") and new military models ("Atrium model" for joint forces). Dr. Demchak has several recent related books: an edited volume entitled Designing Resilience (2010 U Pitt Press with Comfort and Boin) and a theory-to-practice volume Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security Conflicts (2011 UGA Press), as well as a book entitled Military Organizations, Complex Machines in the Cornell Security Studies series. She is currently working on a new manuscript tentatively entitled Organizing for Cyber Security: Cyber Command and National 'Security Resilience' Institutions for a Cybered Conflict Age. She is an early member of the Intelligence and Security Informatics (ISI) research field. As Co-Director of the new Naval War College Center for Cyber Conflict Studies (C3S), Demchak's research will continue to focus on the evolution in socio-technical systems, surprise in organizations, cyber tools, social integrations, and range of choices emerging in westernized nations' cybersecurity/deterrence strategies. Her emphasis remains on comparative operational institutional learning, advanced use of tools and cognition, and system-wide resilience against normal or adversary imposed surprise.

DV - Although several definitions of cyberspace and cyberwar have been proposed (among militaries, governments, researchers), there is no consensus on the definition of this object/concept. What is your own definition of cyberspace and cyberwar?

Ch. D. - Cyberspace is best viewed as a 'substrate' that has grown up underneath our feet and now links every societal process of any significance across modern and modernizing nations. While virtual, it is profoundly a physical phenomenon that humans designed, copied, and adopted widely under a widespread misunderstanding that cyberspace was, and could be, free and safe forever. In fact, the worldwide cyberspace substrate rests on a network of fibre optic cables across land and sea that are purchased, laid down, owned, operated, and maintained by the large telecommunications institutions of modern and modernizing nations. It is a complex, global 'socio-technical' system of unprecedented scale. Its ubiquity of connectivity, ease of use, poor security in design, and low user

cost in access now affect social wellbeing in deeply digitized nations. The same attributes that enhance economies also encourage a massive scale of predatory behaviors that can ripple through social processes in unforeseen ways across far distances without warning.

"Cyber war" is not a helpful term because such a conflict only exists at the far end of the spectrum of likely forms of conflict enabled by cyberspace. A 'cyber war' is an overt, more or less formally declared blend of kinetic and virtual exchanges with uniformed adversaries using cyber means to harm the other sides in the dispute. A 'cyber war' will involve large-scale organizations such as nations who declare their conflict with other states to be active in the same manner a kinetic war is declared. They openly employ all the institutional means at their disposal, including cyber tools or kinetic forces to prevail against their opponents.

Cyberspace as a globally open, nearly free substrate, however, has generated a much wider spectrum of intergroup human conflict than 'cyber war'. In the future, all conflicts of societal significance will be 'cybered conflicts' in that the determining outcomes of these struggles will have seminal events requiring the presence of cyber means in order to occur. The conflict will not stay largely inside networks as in a 'cyber conflict', but will routinely spill out in effects that travel as far and as covertly as the connectivity of cyberspace allows. Indeed, in a generation, the term cybered or cyber will no longer be necessary, because all conflicts will routinely be cybered and the additional term will not be necessary. In the near term, however, we need the term "cybered conflict" to distinguish the differences of these conflicts from traditional state-state struggles. Unlike a cyber 'war', the new form of conflict involves more than states with militaries guided by laws of armed conflict. Rather, this emergent form of conflict engages multiple adversaries on both sides, all of whom are building on the tools, deception operations, patterns of denial, and exploitative innovations of global cybercrime for resources or leverage in the conflict. The normal cybered conflict campaign will involve economic vulnerabilities directly because cyberspace's ubiquitous access allows for the malicious targeting of everything that cyberspace makes accessible from a distance. This conflict is likely to be a long term, continuous, generally masked, and societally comprehensive form of intergroup struggle.

Cybered conflict may break out into an overt "cyber war", but that is not inevitable because that escalation is not really desirable for aggressors. Adversaries of all flavors and motivations will chose deception and denial to critically guide much of their campaign executions because objectives can be more efficiently obtained. If victims across civil society democracies are unable to attribute the effects to the underlying conflict, they are unlikely to develop a consensus to move to the next step of raising the alarm and possible confronting the organized state or transnational sponsors of the campaign. Since avoiding being noticed for as long as possible is a fundamental operational rule in a cybered conflict campaign, digitally open societies can suffer considerable erosion of power and wellbeing in such conflicts for years without knowing or being able to legally prove that they are being deliberately enfeebled. That obliviousness is typical of this new form of conflict in a cybered world but it is much less so for a cyber "war". As cyber-related economic or other crises crystallize into overt exchanges between nations, one knows one is in a cyber 'war'. As of now, however, one 'discovers' that one is in a cybered conflict, and it is often not clear with whom or for how long it has been happening.

DV - If we agree that cyberspace is a new domain, what is a frontier / borderline in it? Is it really necessary for nation-states to set up virtual frontiers? Is such a project feasible?

Ch. D. - Nations build borders for the same reasons we individuals lock the doors to our homes, banks, and cars. Humans will prey upon other humans unless social controls are so institutionalized that this behavior is reduced. In regards to walls and war, nations act like individual humans throughout history, preying upon each other for the resources, the treasures, and the access inside at any time for future leverage. We are now seeing the rise of a "cyber Westphalia" process across the international system to identify the limits of, and tools for, national sovereignty over some part of the cyberspace substrate for the same reasons - to stop loss or prevent worse harm. Leaders of modern and modernizing digital nations are attempting to dampen the overwhelming and massive volume of bad actors reaching easily and daily inside modern nations and draining the nations' wealth and ability to ensure long term national wellbeing.

Such cyber borders are as feasible as any borders ever really are. The cyberspace substrate is completely constructed by humans, and the tools and limits of a national cyber border can be mandated and altered technologically and institutionally within and among nations. The major telecommunications commercial and government-owned privately operated firms ('Telecoms') adopted the relatively simple, insecure, comparatively small, open internet technology developed and funded initially by the US government in the 1990s. They expanded it a thousand of times over to have their proprietary networks become the 'backbone' of the internet inside and outside of nations. Every exchange across cyberspace travels across this substrate because, all along the way, these firms and agencies have negotiated the price and conditions of the exchange of internet data packets with all the other huge telecommunications systems. Ninety-five percent of the internet travels over massive land and sea fibre optic cables run mostly by the same firms that built the national telephone systems. They are largely geographically and nationally circumscribed, and used to being regulated as common carriers. Nations who regulate these telecoms have the structural capacity to jurisdictionally define what is and is not filtered by these institutions, where, how, when, and for what reason.

Furthermore, these national cyber borders may not necessarily be bound to existing physical borders. They can be effectively put in operation anywhere along regulated cable exchanges of the telecom-operated backbones of a nation, and in any form that can be programmed, installed, and monitored. These could be more physical in placing gateways or filters where the undersea cables enter traditional territorial waters or both virtual and physical in being placed where the first major telecom server is entered. Or borders could also be more heavily virtual in that they monitor in depth at many points for particular data structures or patterns, and jurisdictional limits are attached to the content rather than to nodes in the connectivity. Cyberspace is manipulatable at many points, and national political leaders can decide what, where, and how to exert their particular nation's legal controls and sanctions on data transfers to curtail malicious activities passing into their own cyberspace. This is a Westphalian 'process' because it has begun but it will take time both to define and implement those national cyber limits, and to obtain the recognition by other states as part of establishing national cyber sovereignty.

The original Westphalian process took around 400 years and this one will take much less time. Nonetheless, as Pete Dombrowski and I argue in a 2011 article, the 'cyber Westphalian' process will also alter the power and wealth topology of the international system now dependent on the cyberspace

substrate for its overall wellbeing. It is likely that good husbanding of internal national cyber health pushes states to filter what comes into the nation for the good of their citizens, but that 'responsible' cybered state behavior in a cybered era may involve filtered what goes out as well. Today we see the evidence of what is called 'patriotic hacking' en masse, by which hackers inside some nations are not pursued as criminals as long as they hack outside of their home nation. The crystallization of the cyber Westphalian process will include controlling the malicious activity that harms other cybered states. Part of the struggles endemic to the emerging cybered conflict era will be the fight over what a 'responsible' state may allow to emanate from inside their digital jurisdiction. That struggle has already begun with the recent international fights over cyberspace content controls being pursued in the UN ITU.

DV - According to you, what is the most appropriate approach to analyze/explain/understand cyberconflict (ie. its impact on international relations, the origins of cyberwars, etc.): a constructivist approach, a (neo) realist or neoliberal perspective?

Ch.D. - None of these approaches is sufficient because they cannot explain or accommodate the sheer scale or unrelenting nature of the cybered assaults against the open and digital civil societies. Across the web for any reason without compunction or fear of retaliation, attackers in millions can cheaply create cybered conflict campaigns to harm distant strangers over any space of time. Now at low cost, anyone can reach through the cybered substrate to organize an attacking group at any scale, touch at any proximity the data or resources of a large number of victims, and pick a wide variety of targets for any level of precision in attacks. None of these approaches captures the ease of cybered conflict today possible without being a super power or empire or a close neighbor of the targets.

However, taken together, all three approaches do offer tenets about human behavior very relevant to cybered conflict. As I noted in a recent book, their central tenets of belief (constructivism), need (liberal institutionalism), and confidence (realism) can be syncretically combined into a 'theory of action' which offers explanation for the massive explosion of predatory behavior across the cyberspace substrate. In each of these tenets, one finds a driver of decisions to act – that the act be considered legitimate, that it offers a solution to a major life need, and that the actor have confidence of success sufficient to overcome any risks. Put together into a statement that all three must be positively resolved before action occurs, one can then explain why some riot and some do not, the latter often saying it was wrong for them or not worth the gain. The same statement explains the sudden mass move to bad behaviors across cyberspace. The historical psychological constraints against acting to harm someone haven been neutralized by the openness, ubiquity, and near free nature of cyberspace. Legitimacy rarely comes into question, and the need to be met ranges from money to grievances. Confidence is particularly elevated because globally open substrate has also nearly eliminated the scale, proximity, and precision obstacles imposed throughout history by physical geography and the presence of militaries. These latter served to physically and psychologically greatly restrict the volume of would-be attackers. The result is that along with widely enabling malicious surprises from aggressive nations, greed-obsessed transnational organizations, grievance-driven violent groups, and stupidity, cyberspace also adds some considerable portion of adversaries in any cybered conflict who act simply because they now can.

Needed is a combined theory of international relations for the cybered conflict age that builds on the syncretically combined tenets and, especially, the realities of scale, proximity, and precision that only a globally open, unfettered cyberspace substrate can offer. Well resourced adversaries will deftly employ the most skilled elite of the global bad actors in cyberspace, ie, the "wicked actors" ('acteurs insidieux') to pursue the campaigns of gain and leverage that can continue for years below the surface of diplomatic demarches or crises. These persistent attackers will adroitly hide in the masses of regular, poorly skilled criminal or opportunist bad actors. The 'cyber fodder' camouflage can keep the victim groups from realizing their losses over time and raising the alarm for quite some time. Today cyberspace has enabled what the commander of the US Cyber Command has called the "greatest transfer of wealth in human history" from one nation to a major cyber predatory nation with profound implications for cybered conflict between nations. The theory to explain this reality does not yet exist.

DV - What are the main conceptual differences between the 1990s "information warfare" and today s "cyberwar"?

Ch. D. - Information warfare was and still is largely viewed as a military-related activity heavily influenced by its origins in the Cold War. The information warfare concepts of the 1990s are not systemic enough to deal with the emergent, wide variety of cybered conflicts that can occur at many points across the underlying socio-cyber-economic substrate in peacetime. They are evolving today and being absorbed into the emergent field of cybered conflict studies under various labels including cyberspace operations, cyber campaigns, and cyber warfare.

DV - Efforts to conceptualize cyberconflict refer to Cold war and war on terror strategies, policies, concepts (cyber Cold War; cyber deterrence; invisible threat; insider threat;). What is the most appropriate analogy to analyse cyberconflict: Cold war or War on terror?

Ch. D. - Neither captures the unprecedented, wide range of predatory options that cyberspace now offers to a massive, globally dispersed, and uncoordinated population of variously skilled and motivated malicious actors. The 'Cold War' is a term for bipolar or even multipolar states as adversaries. The 'war on terror' is a promotional term used by the United States to indicate seriousness in directly confronting grievance-driven bad actors likely to use terror for political objectives. Predatory behavior involving states and nonstate actors using a globally open cyberspace is often multi-spectrum, involves multiple and diverse sets of actors, and is not confined to motivations of states or political terror. Both states and terrorists can and do use cyberspace in cybered conflicts, but the analogies do not help the national defenders determine how to respond. So many other kinds of actors, tools, and campaigns can and will also be involved at any given time.

Furthermore, both terms are tied to the symbolic connections of militaries and fighting to 'cyber war'. For an emergent era of cybered conflict, a more systemic approach involving resilience and disruption is necessary. Rather than focus on war or non-war, terrorists or non-terrorists, one needs a systemic 'security resilience' response. This strategy is designed for the continuous nature of multi-spectrum cybered conflicts. National leaders continuously weight and adjust strategic packages applying varying information, capital, or coercion tools to foreign populations and actions capable of

using cyber means to harm the homeland, disrupting the action decision of small numbers of well-identified wicked actors working for states or transnational organizations, while simultaneously ensuring national resilience against the harm imposed by the vast scale of other lesser skilled bad actors.

DV - Could you explain why "complexity" is so important in cyberdefense issues? What does the concept mean? What is the impact of complexity on cyberdefense/cybersecurity?

Ch. D. - The cognitive difficulties of the complexity presented by a global scale, open cyberspace substrate that is continually expanding are overwhelming for defenders. In an openly integrated cybered world, defense and offense distinctions blend at the technology level and then migrate up throughout the societal complexities. If some adversary has infected critical supply chains of key computer components across a nation's telecommunications networks, does that constitute aggression, espionage, or crime? Prospective harm is difficult enough to argue in normal security circles; potential harm of this magnitude has proven exceptionally hard to establish. What if one cannot wait for the big hit that proves the vulnerabilities because adverse individual consequences will today cumulate in minutes to hours to produce large systemic impacts?

Furthermore, the normal surprises of complex systems mean these rippling effects can be much more severe and out of control than planned by initiating adversaries. Four layers of increasing complexity imposing surprises now exists across the global cyberspace, each generating ever-higher levels of multi-source surprises. First, the base layer of normal complex surprise generators inherent in largescale complex socio-technical systems (LTSs) such as the individual firm are present across all networked enterprises. Second, when these enterprises connect across regions or domains, one adds a combinatorial layer of complex LTS surprise across the critical infrastructures of regions or nations. Both these base layers would be prone to surprises without the addition of malicious actors. Third, the globally open nature of the cyberspace substrate has added yet another layer of potential surprise, this one created by ease of access inside other nations given to millions of dispersed cybered bad actors throughout global systems by the current topology of cyberspace. Their constant flood of penetration attempt and successes form the vast and overwhelming cognitive challenge today. The final layer, however, is the most pernicious and potentially likely to produce cybered conflict between states. Building on the opportunities for leverage, gain, and long term superiority offered by the lower three layers is a smaller group of exceptionally skilled, persistent, and well resourced group of bad actors called the"wicked actors" (insidieux acteurs). These groups and individuals operate under the cognitive and physical cover of the first three layers, able to exploit the normal surprises of the firm, the shared knowledge failings of the critical infrastructure network, and the constant flood of cybercrime efforts in order to get inside targets.

Complexity is a factor in cybered conflict explicitly because it enables deception and the strategic use of surprise across all the connected elements of any deeply digitized nation. To have or be a credible cyber power, a nation must address the four layers of surprise directly by adopting both resilience and disruption measures in a 'security resilience' strategy. Thee opaqueness and the wide range of possible hostile acts enabled by cyberspace make escalating cybered conflict hard to recognize, and easy to dismiss if one's firm, network, or domain does seem to have yet been personally and directly been hit. The goal of a security resilience strategy is to reduce this cognitive challenge for national leaders and institutions by neutralizing many lower-level generators of complex systems surprise and allowing focus on particularly complex threats.

Complexity across cyberspace makes both resilience and disruption capabilities essential for national cyber power. Resilience across the nation that is so complexly dependent on its digital substrate means an internal systemic ability to collectively anticipate the form or frequency of surprises with serious propagation range and effects, and to prepare to curtail their spread and mitigate their effects immediately. The rise of cyber Westphalian borders will help reduce the floods of remote bad actors and the third layer. However, complex surprises are inherent and can be exploited by anyone. The cyber resilience of a nation requires greater effort domestically to have all public and private actors see their own contributions to, and benefits from, the overall reduction of the systemic vulnerabilities to cybered surprise across all sectors of the nation. This collective recognition of shared dependence needs to deep investments in transparent and 'democratized encryption' and in the underlying transformation of the basic technologies of cyberspace to ensure safety for the whole society using the cyberspace substrate. The second component, forward disruption, will also always be necessary. The use of wicked actors by adversary states or transnational groups will alter as a nation is more resilient but not vanish. The skills of these actors are too advanced for them to be more than inconvenienced or operationally challenged by the rise of cybered borders, casual encryption, and emergent transformations in base layers of cyberspace's technologies. National security against cybered conflict campaigns will also require the ability is to reach forward specifically to disrupt the wicked actors for whom national resilience efforts will is not be sufficient to neutralize their skill and resource advantages. A more systemic approach to accommodating complexity can make it cognitively easier for the defenders of a cyber resilient nation to recognize the conduct of a deliberate cybered conflict campaign at even a low level. Strategically marrying resilience to disruption enables more effective national efforts in neutralizing the benefits complexity affords cybered conflict technologically, societally, institutionally, and strategically over time.