Cyber Westphalia
Asserting State Prerogatives in Cyberspace

Chris Demchak and Peter Dombrowski

Over the last several years, a number of analysts have noticed that states are beginning to seek greater sovereignty over the previously (or perhaps allegedly) ungoverned cyberspace.¹ Research into this phenomenon is only in its preliminary stages. Progress toward understanding how states are responding and adapting to cyberspace has been hindered by definitional complexities, political and ideological positioning, and an absence of data. Moreover, with a few prominent exceptions, the academic disciplines have not focused on the issue.² Over the last three years, however, several scholars including Joseph Nye have published studies that open the door to a new research agenda.³

Speculation about the emergence of the state as a defining player in cyberspace is best viewed as empirically informed theorizing. Since our first use of the term "Cyber Westphalia," the building blocks of what will evolve into cyber borders have emerged around the globe. The frontier era of the global cyberspace ‘substrate’ that increasingly underpins the world’s critical socio-economic systems is thus nearly over. A further transition toward what will eventually be the cybered interstate system is now taking place. During this transition, decisions taken by states — individually and collectively — will

¹ Chris Demchak is a professor at the Naval War College’s Strategic Research Department and founding coDirector of the Naval War College Center for Cyber Conflict Studies (C3S).

² Peter Dombrowski is a professor of strategy at the Naval War College. He is the former head of the Naval War College’s Strategic Research Department.
influence the development of virtual cyber borders. Hence, to what extent are states recreating in cyberspace the older Westphalian process of delineating borders and reaffirming state sovereignty?

This article will first outline the indicators by which progress toward a cyber Westphalian system can be assessed and suggest how these indicators will help us understand patterns of diversity amongst states and non-state actors. These indicators are based on the Westphalian model, ideal-type characterization of what a state is, what a state does, and how states interact to form an interstate system. As with any complex social system, we cannot predict specific outcomes with any confidence, much less the order in which developments will occur. We offer indicators to evaluate how states are, and will, assert their sovereignty. Second, this article will also suggest what progress will look like in the future. We argue that the adaptation of the Westphalian model state to the emergence of cyberspace has been, and will be, a long and fitful process. The transition period will pose the great challenge to citizens/consumer/users, private sector firms, and states seeking to protect themselves from threats ranging from simple malware to sophisticated cyber campaigns intended to undermine governments.

The Westphalian State’s Adaptation to Cyberspace. The modern Westphalian state has been traditionally defined, especially by those in the Realist tradition of international relations theory, by territory, autonomy, control, and mutual recognition. A short article is not the place to provide a detailed examination of the political theories, and historiography underlying the Westphalian model; however, these four basic attributes offer indicative categories by which to assess the broad trends influencing the emergence of a new interstate system. This new interstate system, based in part on a resurgent Westphalian state, will not, in all likelihood, display the same characteristics as in periods prior to the digital information age.

If, as we expect, current states develop for cyberspace the necessary authorities, domestic institutions, and international regimes for exercise political sovereignty, ‘territoriality,’ and non-intervention/mutual recognition, then the existing Westphalian system will have to adapt. Thus, states will have to assert their prerogative over domestic and transnational competitors—ranging from criminal organizations to multinational corporations—while at the same time they reach a modus vivendi with other like-minded, similarly capable states. ‘Territorial’ responsibilities in cyberspace will be assigned, virtual borders established, and normal state-to-state interactions based on mutual recognition and non-intervention will resume where and when possible. Not all states will participate in this process or succeed. A failed state in a deeply cybered world is one that "has a poor capacity to control public order within its territory, is unable to consistently control its borders, cannot reliably maintain viable public institutions or services, and is vulnerable to extra-constitutional domestic challenges ranging from poor levels of economic performance, human welfare, economic distribution, and levels of conflict."
For our purposes here, ‘autonomy’ and ‘territoriality’ are intertwined. The fundamental challenge of where a state’s jurisdictions and responsibilities begin and end is not easily answered with regard to cyberspace. The cyberspace substrate is physical, but also extraordinarily dynamic, prone to complexity, and intensely variable. Autonomy is the ability of a state to impose its will in cyberspace with respect to its own citizens and without regard for the wishes of other states or non-state actors. ‘Territoriality’ defines the edges of jurisdiction over cyberspace that state claims without risking external conflict. If a state is able to alter the cyberspace experienced by its own citizens, and if it recognizes other states’ rights to act in a similar fashion, the state is engaged in defining its own cyberspace autonomy and ‘territoriality’. For example, states such as France and Australia are already creating rules of oversight and procedures with the power of law for their own citizens that are implemented via the existing regulatory controls on national telecommunications firms. By their own practice then, the national telecommunications regulators and firms are slowly becoming the frontline institutions beyond which other states’ or international cyberspace is seen to exist.

‘Control’ for a state in cyberspace means a monopoly on the use of ‘force’ within the society; the legitimacy and even morality of this exercise of control is closely related to the legitimacy and morality of the specific state in question and its underlying governance regime (for example, democratic versus authoritarian). The ubiquitous and largely unbounded nature of the cyber-space substrate both within and outside of states today, however, profoundly challenges traditional notions of the monopoly of ‘force.’ Such control by a state in cyberspace is the ability to prevent or punish harm to society emanating through cyber mechanisms and from sources within the nation. Not only does this attribute imply oversight, coordination, collective action, and management of internal disturbances to critical systems connected by the cybered substrate, it also implies an ability to forestall external cyber-attacks that travel rapidly and non-obviously into the nation. In contrast to the precyber era, ‘force’ is now blurred in terms of tools and authority allocated between, for example, police and military forces.

In cyber terms, a monopoly of force requires more comprehensive capacities within the society to be resilient to cascading cyberspace-related disruptions as well as to be able to forestall (proactively disrupt) particularly harmful adversaries before they penetrate the nation’s traditional physical borders. Thus monopoly of force for a cybered world depends more heavily than prior eras on the ability of the state to develop the resilience and disruptive elements of ‘cyber power’ because the potentially vast scale of attacks and attackers cannot be individually defeated or deterred. For example, states today pursuing resilience or disruption are establishing a variety of institutions to provide often one or the other elements of this monopoly of force. These range or the Computer Emergency Response Teams (or CERTs which were initially private nonprofit organization meant to only provide alerts and mitigating informa-
tion) to the fully proactive agencies aimed at disrupting external threats such as the US Cyber Command.

‘Mutual recognition’ means that states recognize the nascent autonomy, ‘territoriality,’ and monopoly of force claimed by, or de facto established by, other states in cyberspace. Progress has been slow in developing multilateral institutions and frameworks for ordering interstate relations on the full range of cyber issues. As one longtime observer of Internet governance observed recently, “[w]e have one world and we have one Internet, but there are now more than 20 international documents which offer a set of Internet Governance principles.” As a consequence, Internet stakeholders engage in ‘principles shopping’ and other behaviors to avoid laws, rules, regulations, and norms that restrict behaviors in cyberspace. The emergence of rules enforcing mutual recognition of state jurisdictions in cyberspace has been slow because trends in institutional and technological forms of national jurisdiction assertion are not yet converged.

While it seems clear that national-level agencies regulating telecommunications will help demarcate a state’s borders in cyberspace, the process is immature and progress varies widely across states. Several states including China are asserting their own technological sovereignty by designing national Internets connected in limited, protected and channeled ways to the rest of the world. For Germany, its monopoly of control, autonomy, and ‘territoriality’ may rest on relying Germany-only technologies. Russia is defining a ‘.ru’ internal cyberspace only open to Russian citizens; while Russia may rely on the same technologies used by many other states, its logical layers will be adapted to filter, permit, or block what the state defines as its prerogatives. Even though these alternative approaches to defining the nation’s cyber borders are likely to be implemented by the national telecommunications firms and regulatory agencies, each will operate differently to establish what is and is not part of the state in cyberspace.

This article is too short to explore more fully how states are stumbling toward cyber sovereignty under the Westphalian model. Nor can we review the efforts by major and minor nations to impose mutually observed rules for a global cyberspace. However, enough evidence exists to suggest the transition to a cyber Westphalian system is beginning. As examples like those briefly described above accumulate, an increasingly detailed picture of future cybered world complete with cybered conflicts is emerging. To understand these developments conceptually and theoretically, scholars may have to move beyond the framing of mainstream political science, international relations, and security studies scholarship. As Saskia Sassen argues, “writing on the state has tended to focus on the earlier battles to gain territory and the ongoing work of securing the sovereign’s authority over its territory.” In cyberspace and other parts of global economy, critical scholars are recognizing that:

The question of a bordered territory as a parameter for authority has today entered a new phase. States’ exclusive authority over their territory remains the prevalent mode of final authority in the global political economy;
in that sense, then, state-centered border regimes—whether open or closed—remain foundational to our geopolitical. But at least some of the critical components of this territorial authority are actually no longer national in the historically constructed sense of that term. They are, I argue, denationalized components of state authority: they look national but are actually geared toward global agendas, some good, some not so good at all.\(^{14}\)

At this stage our arguments are largely descriptive or perhaps empirical as opposed normative or theoretical in the strong sense used by international relations (IR) theorists. We are not necessarily praising the creation of borders in cyberspace or the reassertion of state sovereignty as positive developments, although both of us agree that states and citizens will accrue some benefits from this process. Nor are we yet in a position to analyze fully the implications of what we document for long-standing debates between various brands of Realism, Liberalism, Constructivism or Post-modernism theories. Admittedly, we have applied categories of ‘stateness’ informed by Realist scholars to begin the process of empirically informed theorizing referenced earlier. Yet, we believe that the Cyber Westphalia phenomenon intersects with, and may influence, Postmodern, Liberal, and Constructivist thinking as well.

**Progress.** The process of establishing cyber borders and thus states’ sovereignty will be nonlinear, dangerous, and lengthy. During the transition, the technical, institutional, and cultural weaknesses of states will be exploited by amoral or criminal individuals, ‘wicked’ actors, unethical or ignorant firms, terrorists and criminal syndicates as well as states not fully committed to an emerging international rule set.\(^{15}\) The lack of linear predictability will force most states to seek more predictability in their international cybered exchanges, though nothing ensures that search will be peaceful or cooperative.

**A Transition Era of ‘Cybered Conflict’**

The transition from now to the point where state authorities gain the upper hand is the period of maximum vulnerability. State interactions are likely to be highly aggressive due to the immense national wealth and power is at stake. Over time, there will be winners and losers all seeking to maintain or change their relative positions. As seen already in Europe and North America already, individual firms and entire industries are vulnerable to hacking on an often-overwhelming scale. For example, Mandiant, an American computer security firm, released a 60-page report detailing hundreds of attacks on American firms and government agencies, many originating from China, dating

---

**The process of establishing** cyber borders and thus states’ sovereignty will be nonlinear, dangerous, and lengthy.
back at least to 2006. Disruptions to day-to-day operations and economic espionage resulting in the theft of valuable intellectual property rights have hit the financial services and defense industries among others.

States have taken increasing notice, not simply because their own information systems are compromised, but because government officials recognize their dependence on the private sector, which has become the weaker link in national security for a deeply cybered nation. This is particularly true for sectors like public utilities and privately provided critical infrastructure where commercial firms hold enormous sway over the economic future of society. The United States is especially concerned with reports that weapons designs and the technical specifications of key military systems may have been compromised. Until proper domestic and legal frameworks have been devised by organized transnational criminals, or by military forces (and often intelligence agencies, law enforcement organizations, and other associated departments), will be present in all types of conflict, during all phases of military or civilian security operations, and intertwined with all the disjointed state-level efforts to define a nation’s cybered prerogatives. The transition period to a cyber Westphalian accommodation will be fraught with complications as all parties to conflict ‘test’ the limits of what effects can, and cannot, be accomplished using cyber operations without escalating into the kinetic exchanges typical of the industrial era ‘war.’

Furthermore, there will be ‘failed states’ in a cybered world—those that do not successfully make the leap to effective authority and capability in cyberspace. Some states will not adapt or will only achieve partial sovereignty—they may establish borders in cyberspace, but lack enforcement tools. Alternately, they might fail to establish effective boundaries, but succeed in building institutions such as cyber commands that are able to project cyberpower. In effect, the signs that a state or group have failed or are failing to adapt to cyberspace are simply the obverse of those signs that powerful, institutionally well-developed states are adapting.

Successful states will wield ‘cyber power’ by demonstrating resilience and disruption capacities in the face of the challenges posed by cybered conflict.

and more resilient socio-technical systems have evolved, states and their citizenry will be vulnerable. Non-state and state actors will attempt to steal the intellectual property needed for economic growth of the victim states.

While we do not think ‘cyber war’ is an immediate threat or, conversely, that cyber war between states is not possible, we argue that all states will face ‘cybered conflicts’ throughout this transition period. From peacetime through high intensity wars, cyber activities whether
challenges posed by cybered conflict. Failed cyber states will either choose not to develop their own domestic laws and organizations—actual and virtual—or try to do so and not succeed. Where in general successful, and failed states will be located within the broader divisions of the international system is not yet clear. We suspect that for obvious reasons Western and Westernized states will have some advantages in navigating the Cyber Westphalian process. The rule of law, institutional efficacy, and a base of material and technological resources bode well for Western or advanced industrial societies. On the other hand, non-Western and/or developing states may have their own, less well understood, advantages. For example, in the coming decades much of the projected growth in cyberspace, in terms of consumers, dollars invested and perhaps even in innovation, will occur outside North America, Europe and Northeast Asia. How this will impact the Cyber Westphalian process remains to be seen.¹⁹

Uncertain Duration

How long the Cyber Westphalia transition will take is unknown; signs of progress are mixed. However, the transition is likely to be at least as long as the frontier era that spanned the last two decades. The underlying technological layer is itself changing as are the social structures depending upon cyberspace. In such a period of uncertain duration, states, firms, and other non-state actors, not to mention citizen-users, resort to a variety of self-help mechanisms, adding to the overall unpredictability of this process. Firms may seek to implement more active defensive measures to proactively and preemptively thwart intrusions. Private vigilantism is common for such transitions, and in cyberspace, can pose threats of escalation and state-on-state engagement, as private actions may be misinterpreted as state action or hypocritically employed as false flags or cover.

In previous eras, major states could shorten the transition by their actions to clarify the ground rules, stakes, and consequences. Although China and the United States seem increasingly willing to discuss mutual cybersecurity concerns, they have not reached agreements able to prevent attacks by each other, other states, criminals, and even terrorists. Many states remain largely outside the existing dialogue about international efforts to regulate cyberspace and diminish cybered conflict, and yet their networks, citizens, and usually impoverished legal systems are directly involved in the generation of threats and disruptions for other states. Furthermore, the United States is no longer the powerful architect and chief arbiter of the existing liberal international system. It will likely have to share leadership of multinational efforts to regulate cyberspace with China and other influential states, regional organizations such as the European Union, and transnational authorities.

The economic and military rise of China as a regional and increasingly global power poses special challenges for the United States and the liberal international presumptions of current global system. Justly or unjustly, many Western analysts believe that Chinese firms, with official backing, have been the most aggressive sources of cybercrime and devastating intrusions into
western government systems, defense industrial firms, and critical infrastructure at a scale far beyond acceptable espionage. Thus, there is unlikely to be a calm acquiescence of China's efforts to influence the emergent cybered international system. After all, attention to cyberspace and insecurities constitute major steps towards institutionalized national autonomy, 'territoriality,' and monopoly of force in cyberspace. The creation of cyber commands or their national equivalent is only one, albeit significant, step in

**In the not-too-distant future,** most states will delineate defensible borders in some measure across the formerly ungoverned, even chaotic cyberspace substrate.

China does not have much experience helping govern the international system by agenda setting and collaboration.\(^5\) This fact alone will complicate the development of enforceable agreements governing cybered conflict and delay the emergence of a set of new international arrangements. Many states will hesitate to concede their own defense when they are not sure what it is they are conceding.

Modern states gradually overwhelmed their institutional competitors: city-states, trading federations, and even empires, and even more slowly imposed rules over international commerce (for example, slavery, finance, and trade) and even interstate war (for example, the laws of war and arms control regimes). Already national cybersecurity strategies are emerging across the major trading democracies along with implementing organizations from national councils able to enforce policies on public and often private actors, to national, but more 'muscular CERTs' able to sense attacks in advance and perhaps interdict them before they are fully executed. National-level agencies with heightened attention to cyberspace and insecurities constitute major steps towards institutionalized national autonomy, 'territoriality,' and monopoly of force in cyberspace. The creation of cyber commands or their national equivalent is only one, albeit significant, step in

That direction. At the current rate of jumbled development demonstrated, we estimate about a generation for the outlines of the new interstate system to emerge.

**A Cyber Westphalia This Way Comes.** In the not-too-distant future, most states will delineate defensible borders in some measure across the formerly ungoverned, even chaotic cyberspace substrate. Whether by accident, mutual adjustments, conflicts, or some combination of all three, states will meet the challenge of cyber threats just as they expanded from the limited competencies implied by Münster and Osnabrück to the full set of functions enjoyed by the modern nation-state. They will legislate the domestic laws giving themselves the necessary authorities, establish the competent military and law enforcement organizations negotiate international treaties, and perhaps even modify existing international organizations to assert controls to the advantage of states. Slowly but surely leading states will take steps, internally and externally, to defend
hard fought prerogatives. One wildcard in this transition is how countries outside North American and Europe exercise their growing market power as cyberspace widens and deepens across the globe. Domestic and international laws and institutions, either entirely new or modified versions of existing organizations will eventually prevail. All these self-interested moves will culminate with a cyber-Westphalian system. Even as we predict that states will adjust to the realities of cyberspace, there are no guarantees that the advantages states enjoyed under the original Westphalian system will be maintained in the future. Near term decisions by individual states to establish their own autonomy, ‘territoriality,’ and control may fail to provide the robust national cyber power needed as the global cyber-substrate changes technologically, socially, and economically during this transition period. More systemic research is needed to understand how states can avoid being left behind as well as how the emerging interstate will reflect a new structural distribution of power.

NOTES


7 Newman, 422.

8 Although as Libicki observes cyberspace consists of three layers: the physical layer, a syntactic layer sitting above the physical, and a semantic layer sitting on top. Martin C. Libicki, Conquest in Cyberspace (Cambridge University Press, 2007).

9 See, for example, remarks by General James Cartwright at the CSIS "Global Security Forum 2012: Fighting a Cyber War" luncheon in which he identifies international cyberspace as the exchange of packets before they are entered into a nation’s national telecommunication system. Available at http://csis.org/event/global-security-forum-2012-fighting-cyber-war


12 "The result has been the emergence of alternative national networks that essentially create alternate domain name systems for in-country use, allowing for censorship of content and stifling the productivity of the current Internet topology. China is one country that has implemented this on a national scale, and Iran is closely following suit." Panayotis A. Yannakogeorgos, "Internet Governance and National Security," Strategic Studies Quarterly (Fall 2012): 119.


14 Sassen, 38.


18 For more explanation of cybered conflict see unpublished manuscript, currently under editorial review, Peter Dombrowski and Chris Demchak, “Cyber war, Cybered Conflict and the Maritime Domain.”

19 For a discussion of the important and somewhat counterintuitive impact of cyberspace into Africa, see, John Reed, “Africa’s Big Brother Lives in Beijing Is Huawei wiring Africa for surveillance? Or just for money?” Foreign Policy Magazine Online (30 July 2013).