CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

Protecting Financial Data in Cyberspace: Precedent for Further Progress on Cyber Norms?

Michael Schmitt, Tim Maurer
Op-Ed August 24, 2017 *Just Security*

Summary: Identifying the legal norms that apply in cyberspace remains highly challenging.

Identifying the legal norms that apply in cyberspace remains highly challenging. The recent collapse of the 5th UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security is an example of the continuing difficulty States are having in agreeing even on foundational principles such as the right of self-defense in cyberspace and the applicability of international humanitarian law during an armed conflict.

In terms of norm identification, few issues have proven more problematic than cyber operations targeting data, whether in peace or war. Of particular note are those involving financial data, in large part because of the interdependency of the global financial system. Responding to this situation, the Carnegie Endowment for International Peace has urged States to pledge to refrain from conducting cyber operations that "undermine the integrity of data and algorithms of financial institutions in peacetime and wartime," as well as the availability of critical financial systems, such as clearing houses. States making the commitment also are asked to agree to respond promptly to another State's appropriate requests for assistance when such incidents do occur.

We believe this proposal has merit in itself. But perhaps as importantly, by building consensus and cooperation on a narrowly defined issue – financial stability – in the face of the current legal drift, the approach could pave the way for broader agreements governing other activities. Here, we outline the legal challenges in applying international law to data-related matters, describe Carnegie's proposal, and reflect on how such an approach could provide a path out of the morass that currently impedes efforts to achieve consensus on legal cyber norms.

Data and International Law

International law, as illustrated in Tallinn Manual 2.0, sets forth a dense web of prohibitions that apply to cyber operations, including those affecting data, during peacetime. The three prohibitions most likely to be implicated by such operations are those involving sovereignty, coercive intervention, and the use of force.

Violations of sovereignty take two forms. First, sovereignty safeguards territorial integrity by, for example, prohibiting remote cyber operations that cause damage to cyber infrastructure on another State's territory or, arguably, significant interference with the functionality of that infrastructure. The manipulation, alteration, or deletion of data could lead to such results, as in causing a SCADA system (a frequently used industrial control system that manages and controls the processes of a plant, machinery, etc.) to malfunction. Second, a violation of sovereignty occurs when a State interferes with, or usurps, another State's inherently governmental functions. An example would be alteration or deletion of data that has been collected for law enforcement purposes.

However, it is unclear whether cyber operations against data that cause effects below the first threshold qualify as violations of sovereignty. Efforts to manipulate the integrity of financial data are unlikely to result in physical damage or loss of functionality of cyber infrastructure (yet could cause a loss of confidence in financial institutions and be highly destabilizing); thus, they exist in this legal grey zone. Similarly, the line between financial activities that amount to inherently governmental acts and those that do not is indistinct. While financial data associated with the State's taxation system, for instance, would be clearly encompassed in the protection, data resident in the servers of State-owned banks might not be.

The second prohibition is that on a State's unlawful intervention into the internal or external affairs of another State. Violation of this prohibition, which was acknowledged by the International Court of Justice in its Nicaragua judgment, requires "coercive" acts related to another State's "domaine réservé." The term coercive refers to acts that either cause a State to engage in activities in which it would otherwise not engage, or refrain from those in which it would take part. Domaine réservé denotes activities that are reserved to the State in the sense of lying outside the realm of international law. The paradigmatic case of a prohibited cyber intervention is manipulation of election returns. In the context of financial data, an operation targeting the integrity of financial data upon which the State pension or welfare system relied in order to compel the target State to adopt a particular domestic policy would exemplify prohibited cyber intervention.

Unfortunately, the notions of coerciveness and domain réservé are less than precise. For instance, a cyber operation that merely draws into question the validity of such data, as distinct from one that manipulates it, would likely engender disagreement over satisfaction of the coercive criterion, whereas it is not certain that a cyber operation directed at the data of a private company that provides State employee pension plans would qualify as an intrusion into the domain réservé.

At the center of peacetime international law lies the prohibition on the use of force found in Article 2(4) of the UN Charter and customary international law. There appears to be fairly widespread consensus, despite the GGE hesitancy, that a destructive or injurious cyber operation directed by one State against another would cross the use of force threshold, and, if severe enough to qualify as an "armed attack," open the door to forceful cyber or kinetic responses pursuant to the customary international law right of self-defense that is reflected in Article 51 of the Charter. There would likewise seem to be agreement that merely destroying data is not *per se* the sort of prohibited action contemplated by the use of force prohibition.

However, debate continues over whether non-physically destructive cyber operations can nevertheless qualify as prohibited uses of force. In particular, there is a strong argument to be made that it is less the nature of the consequences (destructive or not) that matters, than it is their severity. By this approach, a cyber operation targeting financial data that results in, for instance, severe financial instability and widespread economic disruption might amount to a prohibited use of force. But the approach is far from universally embraced, while the threshold that would so qualify a cyber operation as sufficiently severe remains unsettled even among its proponents.

During periods of international armed conflict, the normative framework for the treatment of data is likewise controversial. Three obstacles exist. First, most of international humanitarian law's targeting prohibitions are framed in terms of "attacks," including that which prohibits an attack on civilian objects. In this regard, there is agreement that physically destructive cyber operations qualify as attacks and therefore may not be directed at civilian objects. This would include the alteration or deletion of data that results in physical harm to, or permanent loss of functionality of, the cyberinfrastructure that relies on it. Yet, disagreement exists as to operations that are not physically destructive. In particular, it is not clear that a cyber operation undermining the integrity of financial data, but not affecting the associated cyberinfrastructure, would qualify as an attack and therefore be subject to the prohibition on attacking civilian objects.

Second, there is a lack of agreement as to whether data constitutes an "object," such that the prohibition on attacking civilian objects applies at all. On one side of the debate are those who argue that data is intangible and therefore does not fall, at least not yet, within the plain meaning of the term "object." Others assert the contrary in the sense that, for example, data may be stored, physically transferred on media such as a USB stick, and destroyed (see here and here). The interpretive distinction is critical, for if civilian financial and other data does not qualify as an object, it may be targeted, subject to some narrow exceptions, without violating international humanitarian law.

Finally, assuming solely for the sake of analysis, that data is an "object" that is capable of being "attacked" as a matter of law, the question arises as to which data qualifies as a "military objective" legally susceptible to attack. Clearly, data used for waging war ("war-fighting"), such as that in a command-and-control system or targeting database, would qualify as a military objective. So too would that which

directly supports the war effort ("war-supporting"), as in the case of data essential to the functioning of a munitions plant. However, a long-standing debate surrounds so-called "war-sustaining" objects. The United States takes the view (see para. 5.6.6.2 of the Department of Defense Manual) that the war-sustaining character of an object renders it legally targetable, as with export oil, the proceeds from the sale of which make it possible to maintain the war effort. Many other States, as well as many international humanitarian law experts, are unwilling to extend the notion of military objective this far. The issue has direct relevance in the data context because cyber operations against an enemy's financial system could directly impede its ability to sustain the conflict. Indeed, they likely would do so with greater effect than kinetic or cyber attacks on oil or other resources that indirectly provide the war effort's economic foundation.

Due to such uncertainty during both times of peace and war, international law, at least in respect to data, is simply not up to the task of safeguarding the interdependent domestic, regional, and global financial systems.

The Carnegie Proposal

In the face of this normative ambiguity, Carnegie has proffered its proposal, one responsive to the fact that, irrespective of the correct interpretation of the law, hostile cyber operations affecting the integrity of data of financial institutions, whether during times of peace or armed conflict, can generate devastating consequences far beyond the borders of the State where the targeted financial institution is located. This risk extends to the unavailability of certain systems critical to financial stability. Examples of contagious effects include the impact throughout Asia of the 1997 Thai currency collapse and the global financial disruption spawned by the 2008 collapse of Lehman Brothers, the global financial services firm. Offensive cyber operations could be the trigger for similar crises in the future.

The conduct of such operations during armed conflict similarly could have widespread consequences. This was a lesson illustrated over a century ago in the First World War when the British leveraged their power and influence in the global trade and financial system to conduct economic warfare against Germany. The strategy was abandoned in a matter of months because of its reverberating effects, including on Great Britain. In modern warfare, a cyber operation against a belligerent's financial system is certain to have adverse effects in States that are not party to the conflict. This raises serious questions as to whether such cyber operations would be consistent with the object and purpose of international humanitarian law and the law of neutrality.

Carnegie's proposed agreement is relatively modest in scope. As presently set forth, it is meant only for the G20 States, both because it is there that initial progress is viable and because an agreement among them would have substantial precedent-setting value vis-a-vis other States. Additionally, the agreement would be limited to the financial sector. That sector is a particularly lucrative one for such an approach because the interdependence that characterizes it, albeit rendering the sector especially vulnerable, makes an agreement on its protection a matter of common interest.

Of particular importance is the fact that the proposal covers only the integrity of data of financial institutions and the availability of critical financial systems that could have similarly destabilizing effects. In particular, it does not include a prohibition on conducting cyber operations that simply block access to data for a brief period of time or that violate confidentiality. In Carnegie's view, a correct one in our estimation, the risks associated with manipulation of financial data are far more severe than most operations rendering data unavailable or no longer confidential. As an example, distributed denial of service attacks are temporary and reversible and, with few exceptions, do not pose a significant risk to financial stability. Moreover, the Carnegie proposal acknowledges that there may be situations in which States have a defensible rationale for making certain financial data temporarily unavailable or breaching confidentiality, as in the cases of disrupting terrorist financing or gathering valuable national security intelligence.

The requirement to respond promptly to a request for assistance from another State in case such incidents occur is arguably already found in the principle of due diligence. Admittedly, that principle as applied in the cyber context is somewhat controversial. But even so, it should be noted that the 2015 UN GGE, a body that included all five permanent members of the Security Council, agreed in hortatory terms that that States "should seek to ensure that their territory is not used by non-State actors" for unlawful activities.

Lest States be overly concerned about the agreement's application during an armed conflict, we would caution that it would only encompass the integrity of data and the availability of critical financial systems when an attack thereon would have contagious effects likely to affect financial stability. It would not prohibit, nor would States agree to such a prohibition, the targeting of discrete financial data upon which

the military alone relies. As an example, financial data or algorithms that are unique to the armed forces, such as those algorithms necessary to pay soldier salaries, would be fair game.

A Model for Future Progress?

The success of the proposal could serve as a model for broadening agreement beyond the confines of data of financial institutions. For instance, the UN GGE has repeatedly highlighted the importance of the protection of critical infrastructure. Clearly, an agreement on such matters would be more complex than that described above.

Yet, achieving consensus, for example, on the protection of data upon which healthcare or food and water distribution systems rely would appear to be achievable. A similar logic could apply to the integrity of elections, at least during peacetime. And as to armed conflicts, one of us has proposed that States accept, as a matter of policy, a prohibition on conducting cyber operations against data that underpin "essential civilian functions," such as banking or transportation unrelated to the armed conflict, a suggestion that was later echoed by the International Committee of the Red Cross in an important report on humanitarian law. Of course, defining "essential civilian functions" would be a task no easier than agreeing upon the scope of the term critical cyber infrastructure for peacetime application. But, as in the previous case, agreement regarding individual essential functions would appear plausible. Such agreements would deftly skirt around the legal potholes that characterize the application of international law to data.

The point is that shortcomings in international law should not stand in the way of policy agreement on the protection of those values that are common across societies, whether during peacetime or armed conflict. Such agreements might even mature over time to the point where compliance occurs out of a sense of legal obligation. Should this take place, the norm in question could crystallize into binding customary international law. In light of the intransigence of the community of States to achieve agreement on legal norms, the Carnegie initiative may offer a model for an alternate path leading in the same direction.

This article was originally published in *Just Security*.

End of document

About the Cyber Policy Initiative Program

The Carnegie Cyber Policy Initiative focuses on addressing international cyber policy challenges, as cyberspace is increasingly central to international security and diplomacy. The Initiative develops and promotes norms and policy recommendations for enhancing international stability and security in cyberspace.

Carnegie Endowment for International Peace

1779 Massachusetts Avenue NW
Washington, DC 20036-2103

Phone: 202 483 7600
Fax: 202 483 1840

Contact By Email