Maurer, Tim; Levite, Ariel; Perkovich, George

Working Paper

Toward a global norm against manipulating the integrity of financial data

Economics Discussion Papers, No. 2017-38

Provided in Cooperation with:
Kiel Institute for the World Economy – Leibniz Center for Research on Global Economic Challenges

Suggested Citation: Maurer, Tim; Levite, Ariel; Perkovich, George (2017) : Toward a global norm against manipulating the integrity of financial data, Economics Discussion Papers, No. 2017-38, Kiel Institute for the World Economy (IfW), Kiel

This Version is available at:
https://hdl.handle.net/10419/162579

Economics
The Open-Access, Open-Assessment E-Journal

Discussion Paper
No. 2017-38 | June 23, 2017 | http://www.economics-ejournal.org/economics/discussionpapers/2017-38

Toward a global norm against manipulating the integrity of financial data

Tim Maurer, Ariel Levite, and George Perkovich

Abstract
The financial crisis that erupted in 2007 highlighted how important trust is for the global system and how fragile it can be. The 2016 Bangladesh central bank cyber incident exposed a new threat to financial stability and the unprecedented scale of the risk that malicious cyber actors pose to financial institutions. Beyond theft, using cyber operations to manipulate the integrity of data, in particular, poses a distinct and greater set of systemic risks than other forms of financial coercion. The complex and interdependent character of the financial system and its transcendence of physical and national boundaries mean that manipulating the integrity of financial institutions' data can, intentionally and/or unintentionally, threaten financial stability and the stability of the international system. Importantly, unlike the 2007–2008 global crisis, this risk exists independent of the underlying economic fundamentals and will only increase as more and more governments make cashless economies an explicit goal. The G20 finance ministers and central bank governors should be commended for urging improvements in the resilience of the global financial system in their March 2017 communique. In a next step, the G20 member states could commit their countries explicitly to refrain from using offensive cybertools to corrupt the integrity of data in the financial system and to cooperate when such attacks do occur.

(Submitted as G20 Policy Paper)

JEL F50 F55 G15 H87 K24 K33
Keywords G20; cybersecurity; financial stability; data integrity; financial institutions

Authors
Tim Maurer, ✉ Carnegie Endowment for International Peace, TMaurer@ceip.org
Ariel Levite, Carnegie Endowment for International Peace
George Perkovich, Carnegie Endowment for International Peace

The authors would like to recognize Taylor Brooks, Steven Nyikos, and Elizabeth Whitfield for their assistance on this publication as well as over four dozen officials and experts in more than ten countries for sharing their feedback and insights.

Citation Tim Maurer, Ariel Levite, and George Perkovich (2017). Toward a global norm against manipulating the integrity of financial data. Economics Discussion Papers, No 2017-38, Kiel Institute for the World Economy. http://www.economics-ejournal.org/economics/discussionpapers/2017-38

Received May 18, 2017 **Accepted as Economics Discussion Paper** June 20, 2017
Published June 23, 2017

Introduction

On March 18, 2017, the finance ministers and central bank governors of the world's twenty leading economies—the G20—issued a communiqué highlighting that

> The malicious use of Information and Communication Technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence and endanger financial stability. We will promote the resilience of financial services and institutions in G20 jurisdictions against the malicious use of ICT, including from countries outside the G20. With the aim of enhancing our cross-border cooperation, we ask the FSB [Financial Stability Board], as a first step, to perform a stock-taking of existing relevant released regulations and supervisory practices in our jurisdictions, as well as of existing international guidance, including to identify effective practices. The FSB should inform about the progress of this work by the Leaders Summit in July 2017 and deliver a stock-take report by October 2017.[1]

The G20 finance ministers and central bank governors should be commended for urging improvements in the resilience of the global financial system. But governments should not only ask the private sector to do more; governments themselves can help reduce the risk to the financial sector. The G20 heads of state could commit their countries explicitly to refrain from using offensive cybertools to corrupt the integrity of data in the financial system and to cooperate when such attacks do occur.

The financial crisis that erupted in 2007 highlighted how important trust is for the global system and how fragile it can be. The 2016 Bangladesh central bank cyber incident exposed a new threat to financial stability and the unprecedented scale of the risk that malicious cyber actors pose to financial

[1] G20 Finance Ministers and Central Bank Governors, "Communiqué," University of Toronto, March 18, 2017, http://www.g20.utoronto.ca/2017/170318-finance-en.html.

institutions.[2] Beyond theft, using cyber operations to manipulate the integrity of data, in particular, poses a distinct and greater set of systemic risks than other forms of financial coercion. The complex and interdependent character of the financial system and its transcendence of physical and national boundaries mean that manipulating the integrity of financial institutions' data can, intentionally and/or unintentionally, threaten financial stability and the stability of the international system. Importantly, unlike the 2007–2008 global crisis, this risk exists independent of the underlying economic fundamentals and will only increase as more and more governments make cashless economies an explicit goal.[3]

In 2015, the UN Group of Governmental Experts (UNGGE) and the G20 had already suggested broad norms against attacks on critical civilian infrastructure in peacetime. The G20 finance ministers and central bank governors have now highlighted particularly the risk to financial stability. In this text, we therefore propose that states build on these existing agreements and go further, explicitly committing not to undermine the integrity of data and algorithms of financial institutions in peacetime or during war,[4] nor to allow their nationals to do so.[5]

---

[2] For an extensive review of this and other past cyber incidents involving financial institutions, please see the appendix. Krishna N. Das and Jonathan Spicer, "The SWIFT Hack—How the New York Fed Fumbled Over the Bangladesh Bank Cyber-Heist," Reuters, July 21, 2016, http://www.reuters.com/investigates/special-report/cyber-heist-federal/.

[3] States' reliance on financial data and the system's interdependence is likely to increase. For example, in December 2015, the *New York Times* ran a story about the Swedish government's effort to move the country to an entirely cashless economy, and the UN is supporting countries' efforts toward cashless economies through its Better Than Cash Alliance. The Indian government is also pursuing a cashless economy. See Liz Alderman, "In Sweden, a Cash-Free Future Nears," *New York Times*, April 26, 2015, http://www.nytimes.com/2015/12/27/business/international/in-sweden-a-cash-free-future-nears.html?_r=0; Better Than Cash Alliance, accessed April 21, 2016, https://www.betterthancash.org/; "From Eradicating Black Money to Cashless Economy: PM Modi's Changing Narrative Since Demonetisation," *Indian Express*, December 22, 2016, http://indianexpress.com/article/india/demonetisation-modi-cashless-economy-black-money-narratives-4439843/.

[4] Disk-wiping malware can be included here. Meanwhile, efforts to break cryptography as part of intelligence data collection would not be covered by such an agreement. We also propose that states study the potential inclusion of data availability of certain critical systems as part of such an agreement but recommend exploring this in a follow-up process given the definitional challenges involved.

We propose the following language for such an agreement, of course inviting debate and refinement:

> A State must not conduct or knowingly support any activity that intentionally manipulates the integrity of financial institutions' data and algorithms wherever they are stored or when in transit.
>
> To the extent permitted by law, a State must respond promptly to appropriate requests by another State to mitigate activities manipulating the integrity of financial institutions' data and algorithms when such activities are passing through or emanating from its territory or perpetrated by its citizens.

States have already demonstrated significant restraint from using cyber means against the integrity of financial institutions' data. Such an agreement would therefore be making explicit what could be considered emerging state practice. Making it explicit would

- send a clear signal that the stability of the global financial system depends on preserving the integrity of financial data in peacetime and during war and that the international community considers the latter off limits;
- build confidence among states that already practice restraint in this domain, and thereby increase their leverage to mobilize the international community in case the norm is violated;
- create political momentum for greater collaboration to tackle nonstate actors who target financial institutions with cyber-enabled means; and
- complement and enhance existing agreements and efforts, namely the 2015 G20 statement, the 2015 UNGGE report, and the 2016 cyber guidance from the Committee on Payments and

[5] We are not the first to propose such an agreement but believe that this publication presents the most detailed and comprehensive analysis and proposal to date. For example, Richard Clarke and Robert Knake proposed a similar norm in their 2011 publication; see, Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2011), 269. Greg Austin and Eric Cappon at the EastWest Institute also wrote a short paper on this issue, making the analogy to the 1997 Convention on Crimes against Internationally Protected Persons; see, Greg Austin and Eric Cappon, "Internationally Protected Facilities in Cyberspace: The Examples of Stock Exchanges and Clearing Houses," EastWest Institute, December 2014.

Market Infrastructures and the International Organization of Securities Commissions (CPMI-IOSCO).

While the March 18 G20 finance ministers and central bank governors communiqué does not define "malicious use of ICT," it is reasonable to think that it particularly focuses on the integrity and availability of financial data. For, it is inevitable and not necessarily malicious that law enforcement and intelligence agencies will breach the confidentiality of data in banks and other financial institutions in order to counter terrorism, weapons proliferation, and criminality. This paper therefore describes why it is vital to the stability of the international system to prohibit the corruption of data in the global financial system, and to strengthen a comprehensive norm to this effect.

States would be expected to fulfill these commitments in accordance with the limits and requirements of national and international laws, both of which may ultimately need to be adjusted to reflect the commitments suggested here. They would also be expected to implement existing guidance and best practices, such as those outlined in the 2016 CPMI-IOSCO cyber guidance.[6]

There is now an opportunity for the G20 heads of state to promulgate such a commitment and to ask the Financial Stability Board to implement it in detail, together with the relevant standard-setting bodies, the private sector, law enforcement, and Computer Emergency Response Team (CERT) communities. It would build on the precedent set in 2015 when the G20 decided to include cybersecurity in its head of state communiqué and the precedent with the actions taken by the G20 after the 2007 financial crisis as well as the G20 finance ministers and central bank governors communiqué.

Background

In 2015, the UNGGE, which included representatives from the five permanent members of the UN Security Council, agreed in their consensus report that: "A State should not conduct or knowingly

[6] A moral hazard problem through such an international agreement is theoretically possible but unlikely given the significant threat from nonstate actors. Moreover, pressure to improve resilience through stronger due diligence already exists and an international agreement restraining state behavior would therefore follow and complement such existing efforts.

support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."[7]

This declaration was later endorsed by heads of state at the 2015 G20 summit.8 Such general political commitments are laudable. Yet, history suggests that states often overpromise and underdeliver in upholding such broad normative declarations. One problem is ambiguity: states may differ in how they define critical infrastructure. There is also a growing number of experts expressing skepticism that the UNGGE process will be effective.[9] Moreover, the language developed by the UNGGE focuses on the effects of cyber operations leaving a gap in the specific context of the highly interdependent global financial system. There is value, then, in seeking a more detailed agreement building on and clarifying this language in the context of specific operations that could be especially damaging to the international system.

The financial system is a particularly promising area given existing common interests among most states. It differs from most other types of critical infrastructure, such as transportation or the electrical grid, because it is globally interdependent. Major powers, notwithstanding their fundamental differences, have recognized this in principle and deed. The U.S. government reportedly refrained from using offensive cyber operations against Saddam Hussein's financial systems as well as in hypothetical exercises simulating a conflict with China.[10] Russia's 2011 *Draft Convention on International Information Security* explicitly suggests that "each State Party will take the measures

---

[7] United Nations General Assembly, A/70/174, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, 2015, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement.

[8] "G20 Leaders' Communiqué Antalya Summit, 15-16 November 2015," press release, European Council, November 16, 2015, http://www.consilium.europa.eu/en/press/press-releases/2015/11/16-g20-summit-antalya-communique/.

[9] Joe Uchill, "Israel Cyber Head: US-Backed Cyber Norms Too Broad," *Hill*, September 13, 2016, http://thehill.com/policy/cybersecurity/295651-israel-cyber-head-us-supported-cyber-norms-too-broad.

[10] John Markoff and Thom Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," *New York Times*, August 1, 2009, http://www.nytimes.com/2009/08/02/us/politics/02cyber.html; Clarke and Knake, *Cyber War*, 202–3.

necessary to ensure that the activity of international information systems for the management of the flow of . . . finance . . . continues without interference."[11] China also has a vested interest in the system, reflected, among other ways, by its successful effort to make the renminbi part of the IMF's global reserve currency basket.[12] Meanwhile, countries around the world are setting up or strengthening their CERTs specific to the financial sector, as, for example, India did in February 2017.[13]

Global interdependence makes the financial sector at once more vulnerable than other critical infrastructure and more likely to be in the common interest of states to protect. The damaging effects of an intrusion targeting the electrical grid or the oil and gas sector will be mostly limited to a single country's territory or immediate neighbors. The effects of an incident targeting the data integrity of a financial institution, however, are not necessarily bound by geography. Such effects would be very difficult to understand, and therefore hard to tailor and to predict. An operation targeting a payment processing system could directly corrupt the transactions running through it. Indirectly, a manipulation of the integrity of an institution's data could lead to a bankruptcy that in turn could send shock waves throughout the international system. For example, the 2008 collapse of Lehman Brothers highlighted the unanticipated contagion effect the bankruptcy of even a single institution can have. The 1997 Asian financial crisis was similarly triggered by the collapse of the Thai currency and the unanticipated contagion effect across the region. Such second-order effects are difficult to anticipate. Moreover, they may not be factored in the attacker's battle damage assessments.

International experience in outlawing counterfeiting currencies may be instructive here. States have adhered to and helped enforce the prohibition against counterfeiting because there is widespread

---

[11] Russian Ministry of Foreign Affairs, "Convention on International Information Security," September 22, 2011. http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666.

[12] Mark Fahey and Nick Wells, "Charts: Who Loses When the Renminbi Joins the IMF Basket?," CNBC, December 2, 2015, http://www.cnbc.com/2015/12/02/who-loses-when-the-renminbi-joins-the-imf-basket.html.

[13] Sandhya Dangwal, "Budget 2017: Computer Emergency Response Team to Be Set Up to Check Cyber Frauds," *India*, February 1, 2017, http://www.india.com/news/india/budget-2017-computer-emergency-response-team-to-be-set-up-to-check-cyber-frauds-1802854/.

mutual vulnerability to its effects. And because this restraint is widely accepted, states violating it are highly likely to face punishment. Nonstate actors, of course, persist in counterfeiting, as do North Korea and a few other states, but the practice is contained enough that it does not threaten the stability of the international financial system.[14]

Another historical analogy conveys why major economic powers such as the G20, at least, would have interests in endorsing and upholding a specific norm against manipulating financial data in peacetime and in wartime: in 1914, the British government, using its dominant position in the global trade and financial system, conducted economic warfare against Germany. The strategy succeeded at deranging the global economy but after only three months, the British government abandoned it. The backlash occurred far more intensely and faster than anticipated, including protests from UK businesses, laborers, and political figures and pressure from allies.[15] The then-highly integrated nature of the global economy made it impossible to contain the blowback from an economic attack.

Of course, in the twenty-first century, a few states that are relatively detached from the global economy, and nonstate actors who may or may not be affiliated with them, have capabilities to conduct cyberattacks against financial institutions. Such hostile actors would not be expected to adhere to the proposed commitment. Yet, the states that did endorse such a norm explicitly would be more united and would have a clearer interest and basis for demanding and conducting retaliatory

---

[14] With regard to counterfeiting currency in wartime, the general counsel of the International Monetary Fund, Francois Gianviti, wrote in a 2004 article, "Does the prohibition against counterfeit currency apply in times of war? There have been instances of such practices." For example, Germany's Operation Bernhard targeted the British economy in World War II. The U.S. government reportedly counterfeited Vietnamese and Iraqi currency during its wars with those countries. F. A. Mann, *The Legal Aspect of Money*, 5th ed. (Oxford: Oxford University Press, 1992); "Nazi Fake Banknote 'Part of Plan to Ruin British Economy,'" *Telegraph*, September 29, 2010, http://www.telegraph.co.uk/history/world-war-two/8029844/Nazi-fake-banknote-part-of-plan-to-ruin-British-economy.html; Lizzie Suiter, Jennifer Hucke, and Courtney Schultz, "The War at Home: A Look at Media Propaganda in WWII, Vietnam, and the War in Iraq" (final paper, Stanford EDGE program, December 2004); Youssef M. Ibrahim, "Fake-Money Flood Is Aimed at Crippling Iraq's Economy," *New York Times*, May 27, 1992, http://www.nytimes.com/1992/05/27/world/fake-money-flood-is-aimed-at-crippling-iraq-s-economy.html?pagewanted=all.

[15] Nicholas A. Lambert, "The Strategy of Economic Warfare: A Historical Case Study and Possible Analogy to Contemporary Cyber Warfare," in *Cyber Analogies*, eds. Emily O. Goldman and John Arquilla (Monterey, CA: Naval Postgraduate School, 2014), http://calhoun.nps.edu/bitstream/handle/10945/40037/NPS-DA-14-001.pdf?sequence=1.

action against violators of the norm, be they states, terrorists, or cybercriminals. In other words, the proposed explicit agreement could be a foundation on which to develop collective action against violators of any kind. (Some states that declared adherence could be tempted to tolerate or utilize "privateers" or other proxies to attack financial institutions. But, here, too, the existence of the agreement would provide more leverage than exists today to pressure mal-intentioned states).

Building on Existing Norms and International Law

An explicit agreement against manipulating the integrity of financial institutions' data would build on recent international efforts to develop rules for cyberspace and on foundational international law against counterfeiting currency. Such a commitment also would redress a lacuna in the Law of Armed Conflict (also known as international humanitarian law).

To date, the international community's most important effort to develop rules of the road for cyberspace is the UN Group of Governmental Experts process, whose work was endorsed by the G20 in 2015.

Yet, first, the group's 2015 declaration and its G20 endorsement, thus far, lack detail and concrete steps to turn them into effective and robust security regimes. Second, the UNGGE aspirational norms language applies to peacetime and does not address wartime behavior or the gaps in existing international humanitarian law. It also faces a gap in the specific context of cyber operations targeting financial institutions.

In many ways, manipulating the integrity of financial data is analogous to counterfeiting currency. Here, the 1929 International Convention for the Suppression of Counterfeiting Currency may provide a legal base on which to build.[16] As then general counsel of the International Monetary Fund, François Gianviti, summarized in 2004, "A state's right to issue its currency is protected against foreign states. Therefore, a foreign state may not counterfeit another state's currency (customary international law and Geneva Convention of April 20, 1929 for the Suppression of Counterfeiting

16 More than eighty countries have signed and ratified this convention, with China, India, and the United States among those who have signed but not ratified it.

Currency)."[17] Violations of this prohibition have been rare, demonstrating that the norm has been particularly robust over a period stretching several decades.[18] This reflects states' shared recognition that counterfeiting currency undermines the integrity and trust of the overall financial system on which most, if not all, depend.

However, states have not yet debated and decided whether and how the injunction against counterfeiting could and should be extended to the digital age. That is, can and should the Convention for the Suppression of Counterfeiting Currency be applied to digital currency and/or financial data? If the integrity of financial data in the twenty-first century is as important to maintain as the integrity of currency, then making this explicit through a specific new agreement would serve global interests. The precedent of the anti-counterfeiting regime could foster understanding of this interest and confidence that an injunction against manipulating financial data could be feasible.

The Law of Armed Conflict also currently falls short of accounting for the nature and importance of data. There are at least two large issues here. One relates to *jus ad bellum* (the just cause for war). Legal experts are divided over whether an attack on financial data (however portentous and massive its potential effects) qualifies as a use of force. Article 2(4) of the UN Charter only prohibits the use of armed force, not political or economic coercion.[19] More broadly, with the emergence of hybrid warfare and information warfare, the international community is now wrestling with whether and how to legally treat acts of coercion that fall short of the use of force. The 2017 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* focuses on this issue.

More pertinent is whether *jus in bello* (the just conduct of war) requires or allows data to be judged off-limits from targeting. Legal experts again are divided here. For example, the group of legal experts that compiled the 2013 *Tallinn Manual* argued that data do not constitute an object and that

---

17 Francois Gianviti, "Current Legal Aspects of Monetary Sovereignty," International Monetary Fund, May 24, 2004, https://www.imf.org/external/np/leg/sem/2004/cdmfl/eng/gianvi.pdf.

18 The most recent and well-documented example of a violation of this norm is the superdollar—the counterfeiting by North Korea; Stephen Mihm, "No Ordinary Counterfeit," *New York Times*, July 23, 2006, http://www.nytimes.com/2006/07/23/magazine/23counterfeit.html.

19 Oona Hathaway et al., "The Law of Cyber Attack," *California Law Review* 100 (2012): http://digitalcommons.law.yale.edu/fss_papers/3852/.

therefore offensive cyber operations targeting the integrity of financial data are beyond the scope, principles, and protections of existing international humanitarian law.[20] Consequently, the status of financial data under international law is a subject of debate.

Moreover, whether financial institutions are considered civilian or military objects depends on whether a country defines "military object" narrowly to only include war-fighting capabilities or, as the United States does, broadly to include "war-fighting and war-sustaining" capabilities.[21] In the latter case, financial institutions and their data could be seen as legitimate military targets in wartime (though, as noted earlier, the United States appears to have eschewed such attacks to date).[22]

Thus, an explicit agreement not to manipulate the integrity of financial data could indicate, at least in this narrow domain, how subscribing states intend international law to evolve.

The Proposed Agreement

Current trends in international affairs suggest that cyber threats against infrastructure are most likely to occur in the gray zone between peace and armed conflict.[23] An agreement that only protects the integrity of financial data in peacetime would be insufficient, given how vital the financial system is to the stability and well-being of all states and societies. The potential unintended negative consequences of an attack on the integrity of data, including blowback, weigh heavily against any

---

[20] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 56–57.

[21] For example, the U.S. military destroyed a building in Mosul that housed millions of dollars of currency in January 2016 in an "overall effort to degrade [the Islamic State's] financing." Unlike the previous examples of counterfeiting currency during wartime, this is an example for the destruction of physical currency; Charlie Dunlap, "The Loyola Conference and the Evolving Definition of Military Objective," *Lawfire* (blog), Duke University, February 14, 2016, http://sites.duke.edu/lawfire/2016/02/14/the-loyola-conference-and-the-evolving-definition-of-military-objective/.

[22] One could argue that the U.S. war-sustaining doctrine as such would not need to be changed for such an agreement if it distinguishes between potentially permissible targeting of financial institutions in their physical form but prohibits targeting the integrity of financial institutions' data.

[23] James R. Clapper, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Senate Armed Services Committee, February 9, 2016, http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.

benefit. Moreover, in case of armed conflict, money will be needed to rebuild and to pay any potential reparations. It is therefore desirable and feasible for states to agree not to manipulate the integrity of financial data in any circumstances.

Focusing on the integrity of data does not devalue the importance of protecting its availability and confidentiality. However, it can be argued that the national and international consequences of manipulating data are greater than violations of confidentiality and more difficult to address technically than the interruption of availability. Corruption of data integrity can pose significant challenges for recovery. In addition to technical challenges, certain legal provisions specific to the financial system pose further hurdles, such as settlement finality. For these and other reasons, the manipulation of the integrity of data is a significantly bigger problem than malicious activity undermining the availability of data. Last but not least, while experts might disagree what constitutes "systemic risk" for the financial system, there is widespread consensus that the integrity of data is the most worrisome risk that exists.

Distributed denial of service (DDoS) attacks are relatively common. Technical solutions to prevent and mitigate them are available, and they are temporary and reversible. Moreover, states and the international community (through the United Nations) occasionally impose sanctions on financial institutions, which is somewhat akin to denying availability of the resources in these institutions to their owners and users. Proscriptions of operations that affect the availability of data could be included when the intention and/or effect is to corrupt the integrity of transactions, as in outsider trading, for example. The same applies to the availability of data on certain critical systems. Defining whether and how manipulations of the availability of such data could be addressed and included in the proposed agreement requires broader expert consultation and advice. The G20 should task the Financial Stability Board to work with relevant standard-setting bodies and experts to report on this issue for further consideration.

Regarding confidentiality, some states will continue to conduct cyber operations to gather intelligence from banks and financial institutions. In addition to regulation, such operations are vital to tracking weapons proliferation and countering terrorism, money laundering, drug trafficking, and other illegal

activities. Such espionage is not prohibited by international custom and law.[24] Seeking to proscribe intelligence gathering within a norm against cyber operations targeting financial institutions would make its adoption infeasible and/or raise significant doubts about its effectiveness once in place.

Of course, cyber-intelligence intrusions have motivated other countries to discuss establishing limitations. And technical issues must be addressed to determine whether it could be feasible to distinguish between cyber intrusions of financial systems for intelligence gathering, on one hand, and intrusions designed to enable manipulation of data, on the other hand. The covert installation of payloads capable of affecting the integrity of the financial data would be prohibited.

Taking these considerations into account, the proposed agreement as previously described would have three connected and mutually reinforcing elements:

> A State must not conduct or knowingly support any activity that intentionally manipulates the integrity of financial institutions' data and algorithms wherever they are stored or when in transit.[25]
>
> To the extent permitted by law, a State must respond promptly to appropriate requests by another State to mitigate activities manipulating the integrity of financial institutions' data and algorithms when such activities are passing through or emanating from its territory or perpetrated by its citizens.

These provisions also build on the 2015 UNGGE report's declaration: "States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts."[26]

---

[24] Clarke and Knake, *Cyber War*, 202–3.

[25] For example, by sharing information about a vulnerability with other actors who conduct the malicious action or by turning a blind eye to a nonstate actors' activity.

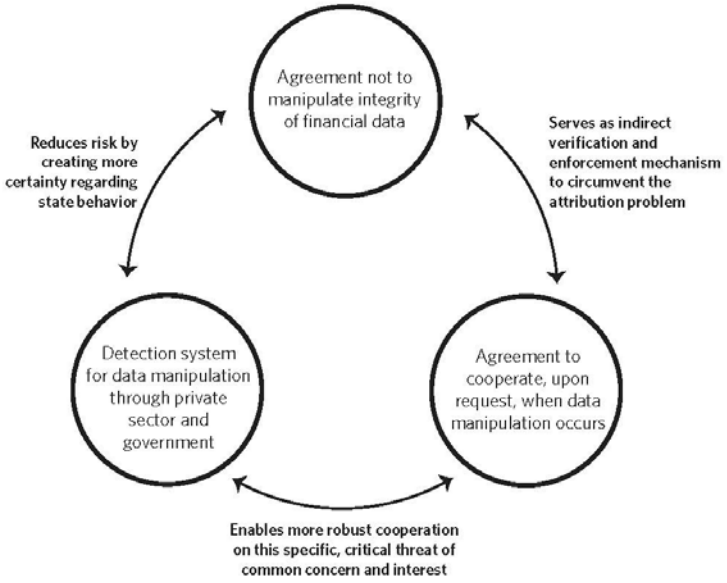
[26] United Nations General Assembly, A/70/174.

The important characteristic of this proposal is that it combines a negative norm, that is, states commit *not to do* something, as well as a positive norm, that is, states commit *to do* something. States would also be expected to implement existing due diligence standards and best practices, such as those outlined in the 2016 CPMI-IOSCO cyber guidance. Linking these three elements would augment the effectiveness of this normative regime overall, as illustrated in Figure 1. Linking the agreement governing state behavior with expectations for the private sector to implement due diligence standards addresses potential moral hazard problems. The commitment by states to provide assistance and information, upon request, circumvents the attribution problem by shifting the burden from the victim of attack to states that profess interest in helping to respond to and ultimately prevent such attacks. States would be expected to comply with these obligations in accordance with the limits and requirements of national and international laws, both of which may ultimately need to be adjusted to reflect the norms described here.

In order to achieve effective reciprocal adherence and be widely accepted among UN member states, the agreement should not be limited to a subset of financial institutions, for example, the Global Systemically Important Banks (as enumerated by the Financial Stability Board) located in a dozen countries. From the standpoint of international stability—and of winning the support of a large number of states—it is worth considering whether protections should be extended to all states' financial institutions. The idea is that cyber operations that threaten the integrity of any financial institution would create precedents and sow fears that could threaten all states.

The envisioned prohibition would be conveyed from states to states. It would not extend to nonstate actors (such as terrorists) operating on territory that the nominal sovereign is unable to police. While a wider scope would be desirable in many ways, practical considerations argue for narrowness. Persuading states to agree will be difficult enough initially, without involving nonstate actors. If and when key states subscribe to something like the agreement proposed here, future work could seek to broaden it in terms of actors and sanctuaried targets.

Figure 1. Three Pillars for an Efective, Self-Reinforcing Regime



Process: Possible Next Steps for Anchoring the Norm

If the proposed agreement is desirable from the standpoint of national and global interests of key states, the question arises where to anchor it, how best to refine the details of its implementation, and where to seek adherents. The G20 has emerged as the most promising forum in which states could address the issues discussed here. One or more such states could champion the idea and invite others to improve upon and support it. Beyond that, the proposal could be raised for consideration in several international forums and multilateral organizations.

If the G20 were to find the proposed agreement compelling, it could:

- Include the language proposed here (or otherwise improved) in the communiqué of the G20 heads of state meeting
- Task the Financial Stability Board to
    - implement and promulgate the agreement with the relevant standard-setting bodies and private sector institutions including CPMI, IOSCO, and the Basel Committee

(this would include exploring some of the questions listed below, namely whether the availability of certain data and systems ought to be included and whether all types of data or specific types of data would fall under the agreement, such as transaction-based data, operations data, and ledger/ownership data); and

- develop a report to be submitted to the next G20 meeting outlining the progress made and a road map for further implementation.

Unlike the actions taken after the 2007–2008 financial crisis, adoption and implementation of an agreement like the one proposed here would require engagement with countries' national security communities and CERTs. No international forum to date exists that allows for such interactions. However, the Financial Stability Board can act as the convener for such a process, potentially working with and supported by other nongovernmental organizations.

The Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions are relevant institutions, especially considering their recent work. The International Monetary Fund is another relevant institution as it is one of the few fora convening both representatives from ministries of finance and from central banks, two important stakeholder groups relevant to this proposal. The World Economic Forum's interest and past engagement with cybersecurity presents an opportunity to raise attention about this issue among top executives from the private sector. These executives would need to be engaged to properly address technical details to enhance the verifiability and robustness of the norm. The Institute of International Finance is another institution that could engage with the global financial industry on these issues.

Finally, there are clearly limits to the extent to which officials in the national security communities of each country can engage with foreign governments and experts in the financial sector. Given that, we can envision a scenario where an international agreement through the G20 would be complemented by a series of unilateral declarations by each government or its military to bolster the G20's statement and contributing to the agreement's effectiveness. Unilateral declarations would also be an easy way for states that are not part of the G20 to express that they join the G20 member states in their commitment.

Questions to Be Addressed

We have developed this proposal with feedback from officials in government, relevant international organizations, and financial institutions in a select number of states, including the United States, Russia, China, the United Kingdom, Singapore, and Israel, to assess its propositions. The feedback has been generally positive; the foundational assumptions outlined in this memo were confirmed or adjusted in subsequent iterations. In order for the norm to be widely accepted and practiced, the following questions would need to be clarified and more fully addressed in its negotiation and implementation. We invite readers to consider them and offer responses to the authors and/or to other interested parties.

1. What should be the scope of financial institutions? Are the definitions and scope listed below sufficient, or would they need to be narrowed or broadened?[27] The following terminology lists already agreed-upon definitions in international trade, especially the final definitions negotiated as part of the Trans-Pacific Partnership (TPP), and the international finance community:
    - "any financial intermediary or other enterprise that is authorised to do business and regulated or supervised as a financial institution under the law of the Party in whose territory it is located" (this is the definition of a "financial institution" in the TPP's final text for financial services);
    - "a financial institution, including a branch, located in the territory of a Party that is controlled by persons of another Party" (this is the definition of a "financial institution of another party" in the TPP's final text for financial services);
    - "any non-governmental body, including any securities or futures exchange or market, clearing agency, or other organisation or association, that exercises regulatory or upervisory authority over financial service suppliers or financial institutions by

[27] "Policy Measures to Address Systemically Important Financial Institutions," Financial Stability Board, November 4, 2011, http://www.fsb.org/wp-content/uploads/r_111104bb.pdf?page_moved=1.

statute or delegation from central or regional government" (this is the definition of a "self-regulatory organisation" in the TPP's final text for financial services);[28] and

- "a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions" (this is the definition of "financial market infrastructure" in BIS/IOSCO 2012 *Principles for Financial Market Infrastructures*).[29]

2. Given the potential significant effect for the system at large if certain data and systems are unavailable, how can availability be added and combined with the focus on the integrity of data in a meaningful framing and description? Also, is there malicious activity targeting availability that affects the integrity of transactions, and, if so, how should this be addressed?

3. In the context of an armed conflict and international humanitarian war, can a distinction be made between targeting financial institutions in their physical form versus targeting their data? In other words, if it is permissible to target a bank with conventional means to destroy currency it physically stores, should it not be permissible to target a bank with cyber means because of the latter's potential collateral damage and blowback potential through offensive cyber operations, in particular?

4. With financial institutions taking advantage of cloud services to outsource part of their data management to other companies, is the proposed language "wherever they are stored" an effective way to capture this trend? Is it necessary?

---

[28] "Chapter 11: Financial Services," in "Trans-Pacific Partnership," Office of the United States Trade Representative, https://ustr.gov/sites/default/files/TPP-Final-Text-Financial-Services.pdf.

[29] Committee on Payment and Settlement Systems, Technical Committee of the International Organization of Securities Commissions, "Principles for Financial Market Infrastructures," Bank for International Settlements and IOSCO, April 2012, http://www.bis.org/cpmi/publ/d101a.pdf, 176.

5. Would the agreement apply only to those states that agree to accept it, or would those that accept the norm be expected to apply its requirements and limitations vis-à-vis states that did not make a reciprocal commitment?

6. More broadly, in the case of any norm that forswears a very specific activity, how do states avoid seeming to signal tolerance of other activities that may also be harmful? Or conversely, isn't a modest norm better than leaving the domain entirely unaffected?

7. When an incident occurs involving the manipulation of the integrity of a financial institution's data, what cooperation are states expected to provide?
    a. What are current gaps in cooperation among computer security incident response teams and among law enforcement agencies?
    b. What information are states expected to share?
    c. Should states be expected to accept joint investigative teams?
    d. Should states be expected to pass new or to amend existing laws criminalizing such activity on their territory and for all their citizens independent of where the activity occurs, if they do not already exist?
    e. Should states be expected to support punitive action through the UN Security Council in case of violations by a state? Does the state need to be a member of the agreement or should the agreement be complemented by a UN Security Council resolution to apply to the entire UN membership?
    f. What best practices among members of the Convention on Cybercrime can be adopted for this narrower type of incident?
    g. What measures beyond existing cooperative mechanisms among members of the Convention on Cybercrime ought to be included?
    h. What could a template incorporating these details look like?

8. Can techniques be developed to detect intrusions that undermine the integrity of financial institutions' data? And can techniques be developed to distinguish between intrusions for intelligence-gathering and those that would also be able to corrupt data?

9. What notification requirements and regime should be in place for states to become aware of such incidents? What protections must exist?

Finally, we acknowledge that other sectors, such as telecommunications and energy, and the integrity of data of other systems are critical for the financial system. However, any agreements covering these sectors are even more complicated to negotiate and to implement effectively. We therefore offer this proposal as the start for what is likely going to be a prolonged process until an effective comprehensive security regime can be put in place.

Table 1: Overview of Some Relevant Entities to Outreach and Engagement

Permanent UN Security Council Members	**Members of the G20**	**Members of the 2014–2015 UNGGE**	**Members of the 2016–2017 UNGGE**	**Basel Committee on Banking Supervision**	**Countries with Global Systemically Important Banks**	**Countries with Global Systemically Important Insurers**	**Members of the G7**
China	China	China	China	China	China	China	
France	France	France	France	France	France	France	France
Russia	Russia	Russia	Russia	Russia			
United Kingdom	United Kingdom	United Kingdom	United Kingdom	United Kingdom	United Kingdom	United Kingdom	United Kingdom
United States	United States	United States	United States	United States	United States	United States	United States
	Argentina			Argentina			
	Australia		Australia	Australia			
	Brazil	Brazil	Brazil	Brazil			
	Canada		Canada	Canada			Canada
	Germany	Germany	Germany	Germany	Germany	Germany	Germany
	India		India	India			
	Indonesia		Indonesia	Indonesia			
	Italy	Italy		Italy	Italy		Italy
	Japan	Japan	Japan	Japan	Japan		Japan
	Mexico	Mexico	Mexico	Mexico			
	Saudi Arabia			Saudi Arabia			
	South Africa			South Africa			
	South Korea	South Korea	South Korea	South Korea			
	Turkey			Turkey			
		Belarus					
		Colombia					
		Egypt	Egypt				

Table 1 continued

Permanent UN Security Council Members	Members of the G20	Members of the 2014–2015 UNGGE	Members of the 2016–2017 UNGGE	Basel Committee on Banking Supervision	Countries with Global Systemically Important Banks	Countries with Global Systemically Important Insurers	Members of the G7
		Estonia	Estonia				
		Ghana					
		Israel					
		Kenya	Kenya				
		Malaysia					
		Pakistan					
		Spain		Spain	Spain		
			Netherlands	Netherlands	Netherlands	Netherlands	
			Switzerland	Switzerland	Switzerland		
				Belgium	Belgium		
				Sweden	Sweden		
			+ Botswana, Cuba Finland, Kazakhstan, Serbia Senegal	+ Hong Kong* Luxembourg, Singapore			

Appendix: A Review of Past Cyber Incidents Involving Financial Institutions

This section outlines significant cyber incidents targeting financial institutions around the world from 2011 until December 2016, with the addition of a few selected important incidents between 2007 and 2011. It is noteworthy that there is no public data that any of the incidents involving the manipulation of the integrity of financial institutions' data appear to involve states; this suggests states are exercising restraint so far, except for the disk-wiping attack against South Korean financial institutions allegedly carried out by North Korea, and perhaps the low–level, distributed denial of service (DDoS) attacks targeting Russian financial institutions in December 2016.

The cyber incidents listed in the table below include defacement of websites, DDoS attacks, and intrusions using more sophisticated malware. The targets of the incidents were mainly banks but also one stock exchange and one payment system, and the countries whose financial sectors were hit include Belgium, Brazil, Estonia, Georgia, Lebanon, Russia, South Korea, Ukraine, and the United States. In many cases, it is difficult to know with certainty who perpetrated the attack, but the suspected attackers range from criminals and hacking groups acting independently, to hackers acting under state sponsorship and states themselves. This review was part of the authors' preliminary research and supported the assumption that states already exercise significant restraint in this area compared to what is technically possible.

Table 2: Shorthand for Cyberattacks and Dates

Shorthand	**Date**
Russian banks DDoS attacks	Late 2016
Bangladesh central bank heist	Early 2016
Belgian National Bank incident	Early 2016
Shanghai Composite Index manipulation (uncertain)	2015–2016
Russian banks theft	Late 2015
Russian currency manipulation	Early 2015
Metel malware attack on Russian banks	2015
Ukrainian Ministry of Finance data breach	Mid 2015
Warsaw Stock Exchange breach	Late 2014
Ukrainian bank data breach	Mid 2014
Carbanak malware attack	2013–2015
Dark Seoul South Korean attacks	Early 2013
JPMorgan data breach	2012–2015
Brazilian banks DDoS attacks	2012, 2014
Brazilian payment system attack	2012–2014
U.S. banks DDoS attacks	2012–2013
Shanghai Composite Index manipulation (uncertain)	Mid 2012
Lebanese Gauss virus infections	2011–2012
South Korean banks attack	Mid 2011
Nasdaq intrusion	Late 2010
Georgian website defacements	Mid 2008
Estonian DDoS attacks	Mid 2007

2016 DDoS Attacks Targeting Russian Financial Institutions

On December 2, the Russian Federal Security Service announced that it had discovered pending cyberattacks intended to impact "a range of major Russian banks" starting from December 5.[30] Servers and command centers purportedly to be used in these attacks were located in the Netherlands and owned by a Ukrainian hosting company named BlazingFast. Its director, Anton Onoprichuk, said he had no information about the asserted attack and that his company was unable to find any malicious data. The Dutch Ministry of Security and Justice said that it was aware its infrastructure could be used for cyberattacks elsewhere, and in a statement noted that "in case . . . a cyberattack does occur on Monday, then it is up to the Russian authorities to decide whether to start an investigation. . . . If desired, they can ask the Dutch investigating authorities for assistance."[31]

On December 9, Rostelecom, Russia's telecom operator, said in a statement that it had blocked DDoS attacks against the five biggest banks and financial institutions in Russia on December 5. They reached a peak volume of 3.2 million packets per second, which is low compared to the volume of other recent DDoS attacks, and the longest lasted a few hours. The statement further noted that part of the DDoS attacks involved a botnet similar to that used in prior weeks against Germany's Deutsche Telekom and Ireland's Eircom, exploiting a vulnerability in home routers.[32]

There was no identification of state actors or perpetrators of the attack, though the Russian Federal Security Service claimed that it was being organized by "foreign intelligence services" and speculation remained that due to the servers' location and

---

[30] "FSB Reports Foreign Special Services Preparing Massive Cyber Attacks," TASS, December 2, 2016, http://tass.com/politics/916315.

[31] Ivana Kottasova, "Russia: Foreign Hackers Are Trying to Take Down Our Banks," CNN, December 2, 2016, http://money.cnn.com/2016/12/02/technology/russia-hack-banks-foreign/.

[32] Ibid.

ownership, this had been an action on behalf of Ukraine.[33] The Russian Federal Security Service stated that it expected the DDoS attacks to be accompanied by text messages, agitating social network publications, and blog statements about a "crisis in the Russian credit and financial system, bankruptcy and withdrawal of licenses of leading federal and regional banks," and that "the campaign [would be] directed against several dozen Russian cities."[34] Presumably, this would be an attempt to create a run on Russian banks, initiating a financial crisis. No evidence exists that such action, complementary to the DDoS attacks, was attempted.

2016 Bangladesh Central Bank Heist

In February, media reported that hackers had breached the network of the Bangladesh central bank and sent thirty-five fraudulent transfer requests to the Federal Reserve Bank of New York, totaling nearly $1 billion.[35] Four of these fraudulent requests succeeded and the hackers were able to transfer $81 million to accounts in the Philippines, representing one of the largest bank thefts in history.[36] A fifth request for $20 million to be sent to an account in Sri Lanka was stopped when a misspelling of the recipient's name, "Shalika Fandation" rather than "foundation," raised suspicions.[37] The remaining transfers, which totaled somewhere between $850 and $870 million, were also stopped before they could be completed.[38]

---

[33] Ibid.

[34] "FSB Reports," TASS.

[35] Steve Herman, "Historic Bangladesh Bank Heist Muddled in Mystery," Voice of America, March 24, 2016, http://www.voanews.com/content/historic-bangladesh-bank-heist-muddled-in-mystery/3252379.html; Rick Gladstone, "Bangladesh Bank Chief Resigns After Cyber Theft of $81 Million," *New York Times*, March 15, 2016, http://www.nytimes.com/2016/03/16/world/asia/bangladesh-bank-chief-resigns-after-cyber-theft-of-81-million.html?_r=0.

[36] Reuters, "Spelling Mistake Prevented Hackers Taking $1bn in Bank Heist," *Guardian*, March 10, 2016, http://www.theguardian.com/business/2016/mar/10/spelling-mistake-prevented-bank-heist.

[37] Gladstone, "Bangladesh Bank Chief," *New York Times*.

[38] Reuters, "Spelling Mistake," *Guardian*.

The hackers had introduced malware onto the Bangladesh central bank's server and deployed keylogger software that allowed them to steal the bank's credentials for the SWIFT system. The hackers also custom-designed a malware toolkit that compromised SWIFT's Alliance Access system and was designed to cover their tracks.[39] This toolkit allowed them to delete records of transfer requests, bypass validity checks, delete records of logins, manipulate reporting of balances, and stop attached printers from printing transaction logs. Although the malware was custom-designed for the theft, the toolkit could potentially be used against other banks in the SWIFT system running Alliance Access software.

The cybercriminals had monitored the bank's routine activity in order to create money transfer requests that appeared genuine and timed the thefts over the weekend in Bangladesh when the Federal Reserve reached out to confirm the transactions, and then it was the weekend in New York when the Bangladesh central bank employees instructed the Federal Reserve to cancel the transactions.

2016 Belgian National Bank DDoS Attack

On February 22, a hacking group called DownSec Belgium shut down the website for Belgium's National Bank for most of the morning using DDoS attacks.[40] Little information has been reported about the attack, but it followed similar DDoS attacks by the same group against the websites for the Belgian Federal Agency for Nuclear Control, the country's Crisis Center, and Belgium's federal cyber emergency team. DownSec Belgium claims to fight against corrupt government abuses.

---

[39] Sergei Shevchenko, "Two Bytes To $951m," *Bae Systems Threat Research Blog*, April 25, 2016, http://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html.

[40] Laurens Cerulus, "Belgian Government Plagued by Hackers," *Politico*, February 22, 2016, http://www.politico.eu/article/belgium-government-agencies-plagued-hackers-downsec-ddos-attacks-cyber-crime/.

2015 Dip in the Shanghai Stock Market (uncertain incident)

Beginning on June 12, the Shanghai Composite Index began to crash, and by June 19 it had fallen by 13 percent.[41] Chinese stock markets continued to fall throughout July and August, and again in January and February 2016.[42] Although there is no public evidence, some have speculated that the sudden crash may have been caused by a cyberattack.[43]

2015 Russian Banks' Thefts From the Banks' Own Customers

There's little information available on this incident currently, but *SC Magazine UK* recently reported that the Russian Central Bank revoked the licenses of three Russian banks in 2015 because an investigation uncovered evidence that current and former bank employees had been using cyberattacks to withdraw money from the accounts of their own clients, as well as to cover up other crimes and violations committed by the banks.[44] The Russian Central Bank reported that in the last quarter of 2015 alone, more than $20 million was stolen from the accounts of clients with what the central bank suspects was the knowledge or direct participation of the banks themselves. The central bank also reported that these hacks were likely the result of huge cuts to the financial industry in Russia over the preceding year, and these cuts had left disgruntled former bank employees willing to collaborate with hackers and left the banks unwilling or unable to shoulder the cost of upgrading their cybersecurity.

---

41 Charles Riley, "China Stocks Plunge as Bubble Fears Grow," *The Open* (blog), CNN, June 19, 2015, http://money.cnn.com/2015/06/19/investing/china-stocks-shanghai-correction/.

42 "Chinese Stocks Tumble for a Second Day After Global Fall," BBC, August 25, 2015, http://www.bbc.com/news/business-34048084; Diane Alter, "What Today's China Stock Market Crash Means for Your Money in 2016," *Money Morning*, February 25, 2016, http://moneymorning.com/2016/02/25/what-todays-china-stock-market-crash-means-for-your-money-in-2016/.

43 AJ Vicens, "The Shocking Truth About Wednesday's Apocalypse Involving Wall Street, China, ISIS, and United Airlines," *Mother Jones*, July 8, 2015, http://www.motherjones.com/politics/2015/07/nyse-glitch-hack-china-cia-cyber-isis.

44 Eugene Gerden, "Russian Bank Licences Revoked for Using Hackers to Withdraw Funds," *SC Magazine UK*, February 17, 2016, http://www.scmagazineuk.com/russian-bank-licences-revoked-for-using-hackers-to-withdraw-funds/article/474464/.

2015 Malware Currency Manipulation Through Russian Bank

Russian-language hackers used a virus called the Corkow Trojan to hack into the computer systems of Russian-based Energobank starting in September 2014.[45] They were able to harvest credentials, launch their own trading software, and, on February 27, 2015, they placed more than $500 million in orders at nonmarket rates that caused the exchange rate to swing with extreme volatility between 55 and 66 rubles per dollar for a period of fourteen minutes.[46] Interestingly, it doesn't appear that the hackers made any significant profit directly from the operation itself, although it's possible that they took advantage of their insider knowledge to profit in other markets. It's also possible that this attack was a pilot exercise for future attacks. Energobank has claimed losses of $3.2 million due to the trades.

2015 Metel Malware Attack on Russian Banks

A group of cybercriminals used the previously discovered Metel banking Trojan to steal directly from banks rather than end users. The criminal gang—which is believed to consist of fewer than ten members—used spear phishing emails or browser vulnerabilities to hack into parts of the banks' systems that had access to money transactions, such as the computers used by call center operators or the banks' support teams. Once inside, the Metel malware automated the rollback of ATM transactions. This allowed the criminal group to use cards from the compromised banks to withdraw a virtually unlimited amount of money, because after each transaction the balance on the account automatically reset to the same amount. No infections of this kind have been detected outside of Russia.[47]

---

[45] Graham Cluley, "Corkow—the Lesser-Known Bitcoin-Curious Cousin of the Russian Banking Trojan Family," We Live Security, February 11, 2014, http://www.welivesecurity.com/2014/02/11/corkow-bitcoin-russian-banking-trojan/; and "How malware moved the exchange rate in Russia," We Live Security, February 12, 2016, http://www.welivesecurity.com/2016/02/12/malware-moved-exchange-rate-russia/.

[46] Jake Rudnitsky and Ilya Khrennikov, "Russian Hackers Moved Ruble Rate With Malware, Group-IB Says," Bloomberg, February 8, 2016, http://www.bloomberg.com/news/articles/2016-02-08/russian-hackers-moved-currency-rate-with-malware-group-ib-says?mod=djemRiskCompliance.

[47] Kate Kochetkova, "Dozens of Banks Lose Millions to Cybercriminals Attacks," *Kaspersky Lab Daily* (blog), February 8, 2016, https://blog.kaspersky.com/metel-gcman-carbanak/11236/.

2015 Ukrainian Ministry of Finance Data Breach

In May, the pro-Russian hacktivist group CyberBerkut claimed to have hacked into the network of the Ukrainian Ministry of Finance.[48] The group posted what it claimed were documents stolen from the network, demonstrating that Ukraine was unable to service its external debt. The veracity of the group's claims and the means by which they allegedly gained access to the ministry's network remain unknown. See the 2014 Ukrainian data breach entry for more information on CyberBerkut.

2014 Warsaw Stock Exchange Breach

In October, a group claiming to be affiliated with the so-called Islamic State hacked the internal networks of the Warsaw Stock Exchange and posted dozens of login credentials for brokers online.[49] The means by which the group gained access to the exchange's networks are unknown, but they were reportedly able to infiltrate an investment simulator and a web portal for managing the stock exchange's upgrade to a new trading system, as well as render the exchange's website unavailable for two hours.[50] Exchange employees say that the trading system itself was not breached. NATO officials later indicated privately that they believed that the hacking group's claim of being affiliated with Islamic militants was a false flag operation, and that in fact the breach was conducted by APT 28, a group widely believed by security researchers to be affiliated with the Russian government.[51]

---

48 "Cyberberkut Hacked the Site of Ukrainian Ministry of Finance: The Country Has No Money," SouthFront, May 25, 2015, https://southfront.org/cyberberkut-hacked-the-site-of-ukrainian-ministry-of-finance-the-country-has-no-money/.

49 Cory Bennett, "Hackers Breach the Warsaw Stock Exchange," *Hill*, October 24, 2014, http://thehill.com/policy/cybersecurity/221806-hackers-breach-the-warsaw-stock-exchange.

50 Michael Riley and Jordan Robertson, "Cyberspace Becomes Second Front in Russia's Clash With NATO," Bloomberg, October 14, 2015, http://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato.

51 Ibid.

2014 Ukrainian Bank Data Breach

In July, the pro-Russian group called CyberBerkut hacked into PrivatBank, one of Ukraine's largest commercial banks, and published stolen customer data on VKontakte, a Russian social media website.[52] The means by which they gained access to the data is unknown. It is believed that they targeted PrivatBank because the bank's co-owner, Igor Kolomoisky, had offered a $10,000 bounty for the capture of Russian-backed militants in Ukraine.[53] CyberBerkut warned PrivatBank customers to transfer their money to state-owned banks. CyberBerkut may have connections to the Russian government, but the relative lack of sophistication of their attacks has led some experts to conclude that official links are unlikely.[54]

2013–2015 Carbanak Malware Attack on Various Banks

A group of criminals used Carbanak malware to attack financial institutions including banks and electronic payment systems in nearly thirty countries. The malware installed a RAT (remote access tool) that allowed the criminals to surveil the banks' daily operations using video feeds and photos over a period of months.[55] The group was then able to order ATMs to dispense cash at terminals and impersonate bank officials to order fraudulent transfers. However, the largest amounts of money were stolen when criminals impersonating bank officers hacked into the banks' accounting systems and manipulated account balances so as to inflate the amount of money available and then transfer the additional money, so that the balance then returned to the original amount. The targeted

---

52 "'Cyber Berkut' Hackers Target Major Ukrainian Bank," *Moscow Times*, July 4, 2014, http://www.themoscowtimes.com/business/article/cyber-berkut-hackers-target-major-ukrainian-bank/502992.html.

53 "Pro-Russian Hackers Mug Key Ukrainian Bank," *ThreatWatch* (blog), Nextgov, July 4, 2014, http://www.nextgov.com/cybersecurity/threatwatch/2014/07/stolen-credentials-network-intrusion-data-dump-pro/1225/.

54 Bill Gertz, "Russian Cyber Warfare Suspected in Bank Attacks," *Flash//CRITIC Cyber Threat News*, August 30, 2014, http://flashcritic.com/russian-cyber-warfare-suspected-bank-attacks-sophisticated-hackers/.

55 David E. Sanger and Nicole Perlroth, "Bank Hackers Steal Millions via Malware," *New York Times*, February 14, 2015, http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?_r=0.

countries included Australia, Brazil, Bulgaria, Canada, China, the Czech Republic, France, Germany, Hong Kong, Iceland, India, Ireland, Morocco, Nepal, Norway, Pakistan, Poland, Romania, Russia, Spain, Switzerland, Taiwan, Ukraine, the United Kingdom, and the United States.[56]

2013 Malware Attack on South Korean Banks

This was an attack on March 20 that used what's known as Dark Seoul malware against the computer networks of three South Korean banks—Shinhan, Nonghyup, and Jeju—resulting in data deletion and disruptions to ATMs and mobile payment systems.[57] Shinhan Bank's internet banking servers were temporarily blocked for part of the day, leaving customers unable to perform online transactions, while operations at some branches of Nonghyup and Jeju were paralyzed for two hours after the virus erased files on the infected computers. A fourth bank, Woori, reported hacking but suffered no damage. Several Korean media organizations were also hit by the attacks: their computers were frozen but they were able to maintain normal broadcasts.[58] South Korea attributed the attack to North Korea.[59]

2012–2015 Crime Ring Responsible for JPMorgan Data Breach

In August 2014, JPMorgan reported a massive data breach in which hackers had gained access to contact information for over 80 million account holders, representing the biggest

---

[56] Kaspersky Lab's Global Research and Analysis Team, "The Great Bank Robbery: The Carbanak APT," *Securelist* (blog), Kaspersky Lab, February 16, 2015, https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/.

[57] Choe Hang-Sun, "Computer Networks in South Korea Are Paralyzed in Cyberattacks," *New York Times*, March 20, 2013, http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html; Juan C. Zarate, "The Cyber Financial Wars on the Horizon," Foundation for Defense of Democracies, July 2015, 1.2–13, http://www.defenddemocracy.org/content/uploads/publications/Cyber_Financial_Wars.pdf,

[58] Hang-Sun, "Computer Networks in South Korea ," *New York Times*; Zarate, "Cyber Financial Wars," Foundation for Defense of Democracies.

[59] K.J. Kwon, "Smoking Gun: South Korea Uncovers Northern Rival's Hacking Codes," CNN, April 22, 2015, http://www.cnn.com/2015/04/22/asia/koreas-cyber-hacking/.

data breach of a U.S. financial institution in history.[60] Although there was initial speculation that the Russian government had been involved,[61] federal authorities indicted four men in November 2015 for the data breach, which they said was part of a huge operation that involved hacking into other financial institutions, a stock-pumping scheme, and online gambling operations that in total had netted them $100 million.[62] The criminals used the email addresses they gained through the JPMorgan hack to run a stock price manipulation scheme and also hoped to set up their own brokerage firm using the stolen data to contact potential customers.[63] Although the JPMorgan hack was their biggest, the crime ring had also hacked six other financial institutions, Scottrade, E-Trade, Dow Jones (the parent company that owns the *Wall Street Journal*), another financial news organization, and several online stock brokerages.[64]

2012 and 2014 DDoS Attacks Against Brazilian Banks

In January 2012, the hacker group Anonymous used DDoS attacks to take down the websites of some of the country's biggest banks, which they said was intended to protest corruption and inequality in Brazil.[65] The attacks, which they dubbed #OpWeeksPayment, shut down the websites for Banco do Brasil, Itaú Unibanco, and Bradesco, among others, for hours at a time.[66]

---

60 James O'Toole, "JPMorgan: 76 Million Customers Hacked," CNN, October 3, 2014, http://money.cnn.com/2014/10/02/technology/security/jpmorgan-hack/?iid=EL; Jose Pagliery, "JPMorgan's Accused Hackers Had Vast $100 Million Operation," CNN, November 10, 2015, http://money.cnn.com/2015/11/10/technology/jpmorgan-hack-charges/.

61 Michael Riley and Jordan Robertson, "FBI Said to Examine Whether Russia Tied to JPMorgan Hacking," Bloomberg, August 27, 2014, http://www.bloomberg.com/news/articles/2014-08-27/fbi-said-to-be-probing-whether-russia-tied-to-jpmorgan-hacking.

62 Kim Zetter, "Four Indicted in Massive JP Morgan Chase Hack," *Wired*, November 10, 2015, http://www.wired.com/2015/11/four-indicted-in-massive-jp-morgan-chase-hack/.

63 Ibid.

64 Ibid.; Pagliery "JPMorgan's Accused Hackers," CNN.

65 Matthew Cowley, "Brazilian Banks' Websites Face Hacker Attacks," *Wall Street Journal*, January 31, 2012, http://www.wsj.com/articles/SB10001424052970204740904577194930748478316?cb=logged0.12500478560104966.

66 Esteban Israel, "Hackers Target Brazil's World Cup for Cyber Attacks," Reuters, February 26, 2014, http://www.reuters.com/article/us-worldcup-brazil-hackers-idUSBREA1P1DE20140226.

In June 2014, Anonymous launched another series of DDoS attacks, this time to protest the World Cup.[67] The attacks, called #OpHackingCup, took down several Brazilian websites including the Bank of Brazil. Other websites that were targeted included Brazilian government websites, Hyundai Brazil, and the official World Cup site.[68]

2012–2014 Malware Attack on Brazilian Payment System

Cybercriminals used "man-in-the-browser" malware to target Boleto Bancario, a popular Brazilian payment system. The payment system allows businesses to issue paper or online *boletos* (tickets) with a barcode that customers can use to remit money at a bank.[69] The malware injected itself into browsers on nearly 200,000 infected computers, where it was able to intercept and alter legitimate *boletos* so as to route payments into the hackers' own accounts.[70] The attack compromised $3.75 billion in transactions, although it is unclear how much of that money the criminals were able to successfully deposit into their own accounts.[71]

2012–2013 DDoS Attacks on U.S. Financial Institutions

These were two coordinated waves of DDoS attacks against U.S. financial institutions' websites, the first in September–October 2012 and the second in December 2012–January 2013.[72] An Islamic hacktivist group called the Izz ad-Din al-Qassam Cyber Fighters

---

67 "#OpWorldCup: Anonymous wages cyber attacks against Brazil govt," *RT*, June 12, 2014, https://www.rt.com/news/165444-anonymous-brazil-world-cup/.

68 Paul Cooper, "Anonymous Lives Up to Threats: FIFA World Cup Hacks Get Underway," IT Pro Portal, June 13, 2014, http://www.itproportal.com/2014/06/13/anonymous-lives-up-to-threats-fifa-world-cup-hacks-get-underway/#ixzz41DPxOwdR.

69 Robert Lemos, "Cyber-Attacks Seen Defrauding Brazilian Payment System of Billions," *eWeek*, July 6, 2014, http://www.eweek.com/security/cyber-attacks-seen-defrauding-brazilian-payment-system-of-billions.html.

70 Eli Marcus, "RSA Uncovers Boleto Fraud Ring in Brazil," RSA, July 2, 2014, https://blogs.rsa.com/rsa-uncovers-boleto-fraud-ring-brazil/.

71 "Boleto Malware May Lose Brazil $3.75bn," BBC, July 3, 2014, http://www.bbc.com/news/technology-28145401.

72 Emilio Iasiello, "Cyber Attack: A Dull Tool to Shape Foreign Policy" (paper presented at the 2013 5th International Conference on Cyber Conflict), 11, https://ccdcoe.org/cycon/2013/proceedings/d3r1s3_Iasiello.pdf.

claimed responsibility for the attacks, which they dubbed Operation Ababil,[73] but U.S. government officials have privately indicated to media that they believe Iran is actually responsible.[74] The scale of the attacks was unprecedented in the number of financial institutions hit and the amount of traffic flooding the sites, with one security researcher commenting that "there have never been this many financial institutions under this much duress."[75] Although the group announced the attacks and the targets in advance both times, the banks were unable to defend themselves and access to the websites of many U.S. financial institutions was disrupted, including Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, PNC, Capital One, Fifth Third Bank, BB&T, and HSBC.[76] Defensive and remedial measures have cost the banks millions of dollars to date.[77] Izz ad-Din al-Qassam Cyber Fighters announced two more waves of cyberattacks in 2013, but they appear to have been less effective.[78]

2012 Possible Manipulation of the Shanghai Stock Exchange (uncertain incident)

On June 4, the Shanghai Composite Index opened at a figure of 2,346.98, and fell exactly 64.89 points by close.[79] June 4 is the anniversary of Beijing's infamous 1989 crackdown on student-led protests in Tiananmen Square, prompting many in China to speculate that

---

[73] David Goldman, "Major Banks Hit With Biggest Cyberattacks in History," CNN, September 28, 2012, http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/.

[74] Barbara Slavin, "US Withholds Evidence for Iran Cyberattacks," *Al-Monitor*, January 17, 2013, http://www.al-monitor.com/pulse/originals/2013/01/cyber-attacks-us-iran-ddos.html.

[75] Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *New York Times*, January 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.

[76] Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," January 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.

[77] Slavin, "US Withholds Evidence," *Al-Monitor*.

[78] Mathew J. Schwartz, "Bank Attackers Restart Operation Ababil DDoS Disruptions," *Dark Reading*, March 6, 2013, http://www.darkreading.com/attacks-and-breaches/bank-attackers-restart-operation-ababil-ddos-disruptions/d/d-id/1108955.

[79] Pete Sweeney and John Ruwitch, "June 4 Crackdown Remembered in China Stock Index, or Chance?," Reuters, June 4, 2012, http://www.reuters.com/article/us-china-stocks-tiananmen-idUSBRE8530F720120604.

both figures may have been intended to represent the anniversary of the tragedy.[80] The number 2,346.98 can be read backwards as the year, month, and date, followed by 23 to represent that 2012 marked the twenty-third anniversary of the protests. Similarly, many observers in China speculated that the 64.89 points that the stock market fell that day also represented 6/4/89. The apparent coincidence led to widespread, but unproven, speculation that the index may have been hacked and manipulated in order to produce those numbers. Numerology is very significant in Chinese culture, and Chinese citizens have been known to use numbers as a subtle form of protest in the past.

2011–2012 Gauss Virus Infecting Lebanese Banks

On August 9, 2012, the Russian security firm Kaspersky Lab announced the discovery of the Gauss virus, which is designed to steal data from Lebanese banks—including the Bank of Beirut, EBLF, BLOM Bank, ByblosBank, Fransabank, and Credit Libanais—as well as from users of Citibank and PayPal.[81] Kaspersky's experts concluded that the virus is state-sponsored malware designed by the creators of Stuxnet, Flame, and the Duqu collection of espionage Trojans.[82] More than 2,500 computers belonging to Kaspersky customers have been infected in twenty-five different countries—1,660 of those in Lebanon—although the security firm cautions that the total number of infected machines may number in the tens of thousands.[83]

Once a PC has been infected, the Trojan steals detailed information, including browser history, passwords, cookies, system configurations, and online banking account

---

[80] Keith Bradsher, "Market's Echo of Tiananmen Date Sets Off Censors," *New York Times*, June 4, 2012, http://www.nytimes.com/2012/06/05/world/asia/anniversary-of-tiananmen-crackdown-echos-through-shanghai-market.html.

[81] "Kaspersky Lab Discovers 'Gauss' – A New Complex Cyber-Threat Designed to Monitor Online Banking Accounts," press release, Kaspersky Lab, August 9, 2012, http://usa.kaspersky.com/about-us/press-center/press-releases/2012/kaspersky-lab-discovers-gauss-new-complex-cyber-threat-desi.

[82] Dan Goodin, "Puzzle Box: The Quest to Crack the World's Most Mysterious Malware Warhead," *Ars Technica*, March 14, 2013, http://arstechnica.com/security/2013/03/the-worlds-most-mysterious-potentially-destructive-malware-is-not-stuxnet/.

[83] Kim Zetter, "Flame and Stuxnet Cousin Targets Lebanese Bank Customers, Carries Mysterious Payload," *Wired*, August 9, 2012, http://www.wired.com/2012/08/gauss-espionage-tool/all/.

credentials, and also installs a special font called Palida Narrow, the purpose of which is unknown.[84] Most interestingly, Gauss contains an encrypted payload that security researchers have been unable to decipher, indicating the presence of a significant exploit that the virus's creators clearly considered important to protect.[85] Given that Lebanon serves as a banking hub for the entire Middle East and that the opacity of the country's banks has often been a concern for financial regulators seeking to disrupt terror financing and money laundering, it seems likely that the virus may be designed to monitor and/or disrupt money flows deemed threatening to the sponsor state's national security.[86]

2011 Malware Targeting a South Korean Bank

This incident targeting the banking operations of Nonghyup, a South Korean agricultural cooperative, began on April 12. The malware initially infected Nonghyup's systems in September 2010 when a subcontractor inadvertently downloaded it onto a laptop, which the attackers used to spread the malware throughout the bank's networks.[87] The attack destroyed the records of some credit card customers and caused a three-day service outage affecting ATMs, online and mobile banking, and credit card usage. South Korea attributed the attack to North Korea.[88]

---

84 "Kaspersky Lab Discovers 'Gauss,'" Kaspersky Lab.

85 Dan Goodin, "Puzzle Box," *Ars Technica*; Kim Zetter, "Suite of Sophisticated Nation-State Attack Tools Found With Connection to Stuxnet," *Wired*, February 16, 2015, http://www.wired.com/2015/02/kapersky-discovers-equation-group/.

86 Zarate, "Cyber Financial Wars," Foundation for Defense of Democracies; Kim Zetter, "Flame and Stuxnet Cousin," *Wired*.

87 Chico Harlan and Ellen Nakashima, "Suspected North Korean Cyber Attack on a Bank Raises Fears for S. Korea, Allies," *Washington Post*, August 29, 2011, https://www.washingtonpost.com/world/national-security/suspected-north-korean-cyber-attack-on-a-bank-raises-fears-for-s-korea-allies/2011/08/07/gIQAvWwIoJ_story.html; "North Korea 'Behind South Korean Bank Cyber Hack,'" BBC, May 3, 2011, http://www.bbc.com/news/world-asia-pacific-13263888.

88 "Prosecution Says N. Korea Behind Nonghyup's Network Breakdown," Yonhap, May 3, 2011, http://english.yonhapnews.co.kr/national/2011/05/03/23/0302000000AEN20110503007100315F.HTML?1a7c6120.

2010 Nasdaq Intrusion

The intrusion of Nasdaq's networks was first reported in an exclusive *Bloomberg Business* exposé in 2014.[89] In October 2010, the FBI detected an intrusion into Nasdaq's computer servers. The intrusion utilized two zero-day vulnerabilities and resembled malware previously designed by Russia's main intelligence agency, the Federal Security Service. The malware first entered through Nasdaq's Directors Desk, a system that hundreds of companies use to share confidential financial information among board members. Nasdaq's own statement at the time reported that the incursion was limited to that system alone, although *Bloomberg*'s reporting indicated that, in fact, the incursion may have spread more widely through the stock exchange's networks while never accessing the trading platform itself.

The NSA initially believed the malware was capable of causing widespread disruption to Nasdaq's computer networks and of possibly wiping the entire exchange. There were also indications that a large cache of data had been stolen, although investigators had little proof of what exactly had been taken. The CIA later argued that the malware was less destructive than originally believed, and that while it couldn't completely wipe a computer system it could take over certain functions and use them to disrupt the network. The investigators ultimately concluded that the intrusion was primarily designed to steal critical proprietary technology for Russia to imitate or incorporate into its own stock exchanges as part of a push to turn Moscow into a global financial hub. The malware has not been publicly analyzed and *Bloomberg*'s reporting included few details, so further technical information about the malware and its capabilities is unavailable in open-source literature.

---

89 Michael Riley, "How Russian Hackers Stole the Nasdaq," Bloomberg, July 21, 2014, http://www.bloomberg.com/bw/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq.

2008 Website Defacement During the Russo-Georgian War

Offensive cyber operations against targets in Georgia began on July 20, prior to the outbreak of the war itself, and continued until mid-August when the conflict ceased.[90] This was the first ever combination of offensive cyber operations with kinetic war and was allegedly carried out by the Russian government or Russian hacktivists with ties to the government.[91] On the day that the kinetic war began, websites sprang up with lists of websites to attack, precise instructions, and survey forms for hackers to report their actions after the fact, demonstrating a telling degree of advance preparation and foreknowledge of the beginning of the conflict.[92] The operations consisted of website defacements and DDoS attacks, with targets including the Georgian president's website and other government sites. The only impact on the financial sector was the defacement of the National Bank of Georgia's website.[93]

2007 DDoS Attacks Against Estonia, Including Estonian Banks

A series of coordinated DDoS attacks against Estonian government, bank, university, and newspaper websites began on April 26, lasting for three weeks.[94] During the first week, the DDoS attacks targeted only government and political parties' email servers and websites, while in the second week the target list expanded to include Estonian news websites.[95] In order to bring their websites back online, network administrators had to

---

90 John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html.

91 David J. Smith, "Russian Cyber Capabilities, Policy and Practice," *inFOCUS Quarterly* 5, no. 1 (Winter 2014): http://www.jewishpolicycenter.org/4924/russian-cyber-capabilities?utm_content=bufferbb5cd&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer; Markoff, "Before the Gunfire, Cyberattacks," *New York Times*.

92 Smith, "Russian Cyber Capabilities, Policy and Practice," *inFocus Quarterly*.

93 Markoff, "Before the Gunfire, Cyberattacks," *New York Times.*

94 Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," *International Affairs Review* 18, no. 2 (2009): http://www.iar-gwu.org/node/65.

95 "Cyberwarfare 101: Case Study of a Textbook Attack," Stratfor, April 18, 2008, https://www.stratfor.com/analysis/cyberwarfare-101-case-study-textbook-attack; Jason Richards, "Denial-of-Service," *International Affairs Review*.

shut them off to foreign traffic, ironically limiting the ability of Estonia's media to tell the rest of the world what was happening.

The third wave of the attack, which began on May 9, was the heaviest yet and focused on the Estonian banking sector.[96] These attacks forced two major Estonian banks—including Hansabank, the country's largest—to suspend online banking operations while also severing the banks' connection to ATMs and preventing customers from using Estonian debit cards outside the country.[97] This wave of attacks was heaviest on May 9–10, and then slowly decreased thereafter until ending on May 19, when the hackers' botnet contracts appear to have expired.[98]

The attacks were carried out by Russian hacktivists communicating openly on Russian-language chatrooms, where users shared precise instructions on how to conduct the attacks. Estonia accused the Russian government of being responsible for ordering the attacks but couldn't produce definitive proof.[99]

96 "Cyberwarfare 101," Stratfor; Richards, "Denial-of-Service," *International Affairs Review*.

97 ""Cyberwarfare 101," Stratfor; Richards, "Denial-of-Service," *International Affairs Review*.

98 "Cyberwarfare 101," Stratfor; Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007, http://www.wired.com/2007/08/ff-estonia/.

99 "Cyberwarfare 101," Stratfor; Davis, "Hackers Take Down," *Wired*.