

Maurer School of Law: Indiana University

Digital Repository @ Maurer Law

Articles by Maurer Faculty

Faculty Scholarship

2015

Hacking the Wealth of Nations: Managing Markets Amid Malware

David P. Fidler

Indiana University Maurer School of Law, dfidler@indiana.edu

Follow this and additional works at: <https://www.repository.law.indiana.edu/facpub>



Part of the [Computer Law Commons](#), and the [International Economics Commons](#)

Recommended Citation

Fidler, David P., "Hacking the Wealth of Nations: Managing Markets Amid Malware" (2015). *Articles by Maurer Faculty*. 2140.

<https://www.repository.law.indiana.edu/facpub/2140>

This Article is brought to you for free and open access by the Faculty Scholarship at Digital Repository @ Maurer Law. It has been accepted for inclusion in Articles by Maurer Faculty by an authorized administrator of Digital Repository @ Maurer Law. For more information, please contact rvaughan@indiana.edu.



LAW LIBRARY
INDIANA UNIVERSITY
Maurer School of Law
Bloomington

HACKING THE WEALTH OF NATIONS: MANAGING MARKETS AMID MALWARE

Cybersecurity has become a major problem in the political management of global economic activities. This article examines how cybersecurity emerged as a challenge in global political economy. The post-Cold War global spread of the Internet and digital technologies happened largely without companies and countries worrying about threats to information, software, and network security. However, as dependence on cyber technologies grew and as conditions in international politics changed, cybersecurity became a serious problem that adversely affects international economic relations. The article also considers the prospects for improved cooperation on cybersecurity within global political economy.

David P. Fidler*



TURKISH POLICY
QUARTERLY

Summer 2015

* David P. Fidler is James Louis Calamaras Professor of Law at the Indiana University Maurer School of Law and an Adjunct Fellow for Cybersecurity at the Council on Foreign Relations, Washington, DC.

The rise of cybersecurity as a policy challenge is a multifaceted global phenomenon. States debate how the security of digital technologies affects cyberspace, geopolitics, armed conflict, international law, and human rights. Cybersecurity has also become an issue in global political economy, or the political management of global economic activities. Breaches of computer systems generate economic costs individuals, companies, and governments bear, including the costs of defending against cyber threats. But, even though substantial, these costs do not tell the whole story about how cybersecurity affects global economic relations.

Cybersecurity emerged as an issue in global political economy through two phases. After the end of the Cold War, a convergence of political, economic, and technological factors stimulated the integration of Internet-linked technologies into economic activities and the globalization of this behavior. These developments happened without the security of digital data, software, hardware, and computer networks becoming a major issue for companies or governments. However, growing dependence on insecure technologies produced significant cybersecurity problems. This phase revealed that cyber vulnerabilities were embedded and globalized in ways that undermine economic benefits associated with digital technology and harm economic relations among states.

The threat includes not only the costs companies and economies suffer from malevolent cyber activities but also the impact of government policy on cybersecurity dangers. Governance actions reflect different understandings of cybersecurity and produce fragmentation in measures affecting the private sector. As a result, the political management of global economic affairs confronts problems related to national policy responses to cybersecurity threats.

The next phase is unfolding as countries formulate ways to advance the global economic benefits associated with cyber technologies while addressing cybersecurity. States are trying to balance the liberalization of digital commerce with the protection of national security and to cooperate on strengthening national cyber defenses. The need to calibrate economic and security interests is familiar in global political economy, but how well governments accomplish this task concerning cybersecurity remains to be seen.

Cyberspace and Global Political Economy

A Remarkable Convergence

The study of global political economy uses economic and political analyses to understand how state and non-state actors organize transnational economic activities.¹

¹ Robert Gilpin, *Global Political Economy: Understanding the International Economic Order* (Princeton: Princeton University Press, 2001).

Technology has long been important to the governance of international economics. Trade and investment liberalization facilitates cross-border flows of technology and its economic benefits, but political problems also arise. During the Cold War, developing countries demanded greater access to advanced technologies, and capitalist states sought to prevent exports of technologies of national security importance to socialist nations.

Explaining how cybersecurity affects global political economy begins with understanding how the technologies responsible for cyberspace spread globally. In political economy terms, getting countries to liberalize trade and investment required intergovernmental agreements, as reflected in the World Trade Organization (WTO) and bilateral investment treaties. This governance architecture proved necessary to create the benefits liberalized trade and investment can produce, including those associated with technological innovation. By contrast, the Internet became a global economic juggernaut without needing such architecture. How did this happen?

“Cyber technologies came of age during unprecedented global political and economic changes.”

Cyber technologies came of age during unprecedented global political and economic changes. First, the Cold War had ended, leaving behind the rigid, ideology-riven bipolar structure that fragmented post-World War II international economic governance. This development opened space for trade and investment to expand. Second, the US emerged as the most powerful country, and US interests favored globalization. Third, countries reformed the trade system through the WTO, which made liberalized trade prominent in economic globalization.

Although not specific to any technology, these developments created political and economic conditions conducive to the global spread of the Internet and related digital technologies as these became increasingly accessible and useful from the mid-1990s. The Internet’s diffusion faced no security constraints related to the balance of power, was propelled by the dominant country, and was supported by governance reforms that liberalized economic relations among nations. In global political economy terms, what happened was a remarkable convergence of technological innovation, political transformation, and economic liberalization.

In another unprecedented feature of this period, the Internet went global without the involvement of mechanisms established to oversee international communications.

Previous technologies, such as the telegraph, radio, and telephony, were subject to international institutions and regulation. After World War II, such governance occurred through the UN's International Telecommunication Union (ITU), an institution that began as the International Telegraph Union in 1865.² However, the ITU did not manage the Internet's expansion or regulate it. Nor did it determine how the Internet functions. Instead, a "multi-stakeholder" process involving academics, companies, non-governmental organizations, and government representatives governs the Internet.³ The post-Cold War convergence of technology, politics, and economics facilitated the extraordinary governance associated with the Internet's spread.

"The post-Cold War convergence of technology, politics, and economics facilitated the extraordinary governance associated with the Internet's spread."

The speed and scale at which the Internet globalized demonstrated that it created benefits for commercial enterprises, including increased efficiency, competitiveness, productivity, market access, and innovation. These incentives powered the digital economy's emergence. As more businesses harnessed online strategies, being offline ceased to be viable, and Internet-based business models generated a multiplier effect across

markets. The manner in which the Internet was disseminated facilitated widespread exploitation of these firm-level advantages.

During the Cold War, international political economy included analyzing rival capitalist, socialist, and developing-world perspectives on economic relations.⁴ Such competition did not affect the emergence of cyberspace and the process of digital globalization. These developments became intertwined with liberal political and economic thinking. The Internet became integral to market liberalization, economic interdependence, democracy, and individual rights. The Soviet Union's collapse ended socialism's ability to compete as an ideology, and developing countries focused on integrating with global markets and shrinking the "digital divide" rather than railing against the impoverished periphery's dependence on the wealthy, exploitative core.

2 "Overview of ITU's History," *International Telecommunication Union (ITU)*, www.itu.int/en/history/Pages/ITUHistory.aspx

3 Wolfgang Kleinwachter, "The History of Internet Governance," in Christian Moller and Arnaud Amouroux (eds.), *Governing the Internet: Freedom and Regulation in the OSCE Region* (Vienna: OSCE, 2007), pp. 41-64.

4 Robert Gilpin, *The Political Economy of International Relations* (Princeton: Princeton University Press, 1987).

The Absence of Cybersecurity

Missing from this narrative is cybersecurity. Generally, the security of information on, and traveling among, networked computer systems did not, in this formative period, attract the policy attention that commercial exploitation of digital technologies generated. The Internet was engineered with openness and accessibility, not security, as primary objectives. The development of software, including applications to run on the Internet, also happened without much consideration given to information, product, or network security.

Cybersecurity concerns that arose did not factor significantly in the emerging global political economy of the digital age. US policymakers identified the need to protect national critical infrastructure from terrorist cyber attacks,⁵ and the Council of Europe negotiated the Convention on Cybercrime to address criminal activities in cyberspace.⁶ Some governments began to think about military applications, such as using cyber weapons in armed conflict.⁷ These examples reveal policy concerns about cybersecurity, but the concerns were not strong enough to divert the trajectory of economic activities becoming dependent on cyber technologies.

“US accusations against Chinese cyber espionage targeting US companies and government agencies have contributed to souring Sino-American relations.”

A different perspective on cybersecurity also appeared in this period. US and European interest in cyber terrorism, cyber crime, and cyber weapons focused on the vulnerability of information, software, and networks. However, Russia and China worried that US political, economic, technological, and military dominance in cyberspace posed security threats beyond vulnerabilities in digital technologies. This broader reading of cybersecurity connected the new realm of cyber to traditional geopolitics. For example, Russia tried through the UN to advance proposals based on its interests, but these efforts did not gain traction because the dominant power, the United States, opposed them.⁸

5 Presidential Decision Directive/NSC-63 on Critical Infrastructure Protection, 22 May 1998.

6 Convention on Cybercrime, *Council of Europe*, European Treaty Series No. 185, 23 November 2001, <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>

7 An Assessment of International Legal Issues in Information Operations, *U.S. Department of Defense Office of General Counsel*, (May 1999).

8 Dorothy Denning, “Reflections on Cyberweapons Control,” *Computer Security Journal*, Vol. 16, No. 4 (Fall 2014), pp. 43-53.

Cybersecurity as a Problem for Global Political Economy

Cybersecurity Emerges

Although marginal to global political economy in this formative period, cybersecurity – in its technological and geopolitical meanings – subsequently emerged as a major issue in global economic affairs. Cybersecurity now features prominently in important economic relationships, such as between the US and the EU, and the US and China. Cybersecurity problems affect efforts to advance trade and investment liberalization, including in negotiations on the Trans-Pacific Partnership (TPP) and Trans-Atlantic Trade and Investment Partnership (TTIP) agreements. The need to address cybersecurity also arises in development activities to facilitate utilization of digital technologies by developing countries.

This change flows from transformed circumstances in global political economy, including at the enterprise level, in markets for digital goods and services, and in the global balance of power. Put simply, awareness of cybersecurity vulnerabilities and their economic costs and political implications increased while policy responses to these problems fragmented in ways that threaten the Internet's role in global economic activities.

As noted above, the digital revolution unfolded without much attention paid to the security of information, software, networks, and Internet-enabled transmissions. This marginalization of cybersecurity reflected market and governance failures that criminals, terrorists, and governments began to exploit on a massive scale, which generated escalating economic costs and political problems. Cyber crime grew in scale, severity, and sophistication. Governance efforts at national and international levels have not kept pace. Despite being open for adoption since 2001, only 46 countries have joined the Convention on Cybercrime. Terrorists use the Internet for multiple purposes, including communication, propaganda, and recruitment, but law enforcement and intelligence responses to terrorist use of the Internet create costly challenges for companies. States have taken advantage of cybersecurity vulnerabilities to engage in extensive cyber surveillance and espionage against foreign nationals, companies, and governments, practices that have caused serious problems between countries.

Government surveillance and espionage have caused the most damage in global political economy terms. US accusations against Chinese cyber espionage targeting US companies and government agencies have contributed to souring Sino-American relations. Disclosures by Edward Snowden, a former contractor for the US National Security Agency, made matters worse because they revealed US operations against Chinese companies (e.g., Huawei) and government targets. Snowden's disclosures also damaged US-EU relations because they included information about US spying

against European nationals, politicians, and companies. The European Parliament threatened to withhold support from the TTIP agreement unless the US met EU demands, including on privacy.⁹

Data Localization and Policy Fragmentation

The Snowden revelations produced interest by governments in data-localization requirements that mandate companies to store data within the country, rather than transmitting and storing the data elsewhere.¹⁰ This development reflects security, privacy, and commercial issues arising from the global dominance of US cyber companies. From a security perspective, this dominance means that information generated inside a country often flows through the US, and, thus, is vulnerable to US government access. For some countries, such access also raises worries that cross-border data flows dilute privacy protections for personal information. Finally, data localization could give domestic companies more business opportunities rather than having US enterprises dominate digital commerce.

“One consequence of the Edward Snowden disclosures was global blowback against US tech companies for being perceived as complicit with US surveillance and espionage.”

Interest in data localization highlights that responses to cybersecurity vulnerabilities exhibit fragmentation through emphasis on national measures rather than collective action. In this vein, China has used Snowden’s disclosures to advance Chinese “techno-nationalism,” impose cybersecurity requirements on foreign companies, and emphasize Chinese sovereignty over the Internet and cyberspace. In the wake of Snowden’s leaks, the EU has insisted that the US government and US-based companies meet its data-protection standards for information concerning EU nationals. The EU has proposed regulations to require commercial enterprises in the common market to strengthen cybersecurity.¹¹ US and European political leaders are increasingly demanding that social media companies do more to combat terrorist use of their services.

⁹ On the Snowden disclosures, see: David P. Fidler (ed.), *The Snowden Reader* (Bloomington, IN: Indiana University Press, 2015).

¹⁰ Karen Kornbluh, “Beyond Borders: Fighting Data Protectionism,” *Democracy: A Journal of Ideas* (Fall 2014), www.democracyjournal.org/34/beyond-borders-fighting-data-philip?page=all

¹¹ Proposal for a Directive of the European Parliament and of the Council concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union, *European Commission*, COM (2013) 48 final, 7 February 2013.

The Problem of US Tech Dominance

A thread running through responses to cybersecurity threats is the dominance of US-based companies in digital commerce. For governments around the world, this dominance makes these companies critical to law enforcement and intelligence efforts to combat crime, counter terrorism, and address other security challenges. One consequence of the Snowden disclosures was global blowback against US tech companies for being perceived as complicit with US surveillance and espionage. Given the importance of global markets, these companies sought to restore customer confidence by, among other things, strengthening the use of encrypted communications. This move sparked controversy, as the US and other governments warned about the threat encryption poses to law enforcement and intelligence efforts in a cyber-dependent world.¹²

“Consensus on regulating economic cyber espionage to address the damage it inflicts on companies and diplomatic relations is not likely.”

Although dominance of US tech companies increases vulnerabilities to US spying and creates incentives for data localization, cybersecurity is also a fig leaf obscuring other reasons why countries chafe at this dominance. From a global political economy perspective, the Internet’s globalization has not produced competitive markets for Internet services. In theory, technology diffusion should increase competition among firms selling goods and services. In practice, US companies have repeatedly become the dominant enterprises. This phenomenon has occurred in the EU’s common market so frequently that the EU increasingly resorts to competition law to accuse US tech companies of abusing their dominant positions. Other countries, such as India and Brazil, are also using competition law to address the market power of US tech enterprises. This turn to competition law creates problems in political and economic relations with the United States.

Geopolitical Changes and Authoritarian Cybersecurity

Cybersecurity’s rise in global political economy also connects to changes in the distribution of power in the international system. During the Internet’s globalization, US power was unmatched and largely unchallenged. This hegemonic status helps explain why the US could brush off Russian and Chinese efforts to shape

¹² Spencer Ackerman, “FBI Chief Wants ‘Backdoor Access’ to Encrypted Communications to Fight ISIS,” *The Guardian*, 8 July 2015, www.theguardian.com/technology/2015/jul/08/fbi-chief-backdoor-access-encryption-isis

cyberspace and Internet governance at the end of the 1990s and beginning of the 2000s. However, as the first decade of the new century progressed, American hegemony receded, and China and Russia began to challenge the US. Chinese and Russian attempts to bring Internet governance more under governmental and intergovernmental control scored a coup in 2012 at an ITU conference that adopted, over US opposition, revised international telecommunication regulations that, for the first time, included cyber elements.¹³

Chinese and Russian assertiveness reflects not only shifts in the balance of power but also increasing confidence by authoritarian states in their ability to handle challenges posed by the Internet. As noted above, the prevailing narrative in the post-Cold War period linked the Internet with free markets, democracy, and human rights. In the crosshairs of this perspective were non-democratic states. However, many authoritarian governments defied expectations by increasing Internet usage among their populations and their control over cyber activities.¹⁴ Driving such control is a broad reading of cybersecurity that justifies extensive government interference in individual and private sector Internet use and, thus, emphasizes sovereignty over liberalized communications, cross-border data flows, and digital commerce.

Cybersecurity and the Digital Divide

Cybersecurity has also become part of development thinking about the digital divide. With high- and middle-income economies experiencing cybersecurity problems caused by dependence on networked digital technologies, advocacy for developing countries to adopt these technologies for economic growth can no longer overlook cybersecurity. As one expert argued, “attempts to reduce the digital divide through investment in infrastructure only, without taking into account the need for security and control of IT risks (...) would result in the creation of a security divide as prejudicial as the digital divide.”¹⁵ The African Union’s negotiation of the Convention on Cyber Security and Personal Data Protection reflects awareness that African governments have responsibilities to address security vulnerabilities that come with cyber-driven development.¹⁶

Global Political Economy and Managing Cybersecurity

With cybersecurity now a major issue in global economic relations, will companies and countries devise better ways to manage this challenge? The seriousness of this problem arose from market and governance failures to address the

¹³ David P. Fidler, “Internet Governance and International Law: The Controversy Concerning the Revision of the International Telecommunication Regulations,” *American Society of International Law Insights*, 7 February 2013, www.asil.org/insights/volume/17/issue/6/internet-governance-and-international-law-controversy-concerning-revision

¹⁴ Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: Public Affairs, 2011).

¹⁵ Solange Ghernaouti, *Cyber Power: Crime, Conflict and Security in Cyberspace* (Lausanne: EPFL Press, 2013), p. 341.

¹⁶ African Union Convention on Cyber Security and Personal Data Protection, EX.CL/846 (XXV), 27 June 2014.

vulnerabilities dependence on cyber technologies produces. Although companies are more aware of the dangers, the private sector continues to struggle in balancing incentives for harnessing technological innovation and the need for greater information, software, and network security. New services, such as cloud computing, are claimed to offer better cybersecurity. However, technological fixes will not solve the problem, especially when innovations on the horizon, such as the Internet of Things and Internet-linked commercial drones, potentially exacerbate cybersecurity threats. As described above, most government responses to cybersecurity problems have been domestically focused, reflect different perspectives on what cybersecurity means, and are fragmented along national lines rather than coordinated through collective action. The need for better cooperation is apparent, but prospects are mixed, at best.

Consensus on regulating economic cyber espionage to address the damage it inflicts on companies and diplomatic relations is not likely. Nor do credible options exist to reduce political and economic tensions associated with major countries, especially China and Russia, exercising Internet sovereignty more vigorously. The economic cyber espionage and Internet sovereignty issues are intertwined with geopolitical problems characterizing US-Russia and US-China relations, which makes cooperation on cybersecurity all the more difficult.

From a global political economy perspective, negotiations to liberalize trade and investment are more interesting. Many countries are participating in efforts to conclude agreements that would liberalize trade in information technology products, trade in services utilizing cyber technologies, and digital commerce. E-commerce provisions in the proposed TPP agreement include not only traditional obligations (such as non-discriminatory treatment) but also new rules on ensuring cross-border data flows and restricting data localization requirements.¹⁷ If accepted, such rules could be an important development in efforts to liberalize economic activities that harness the potential of cyber technologies.

Negotiating rules on cross-border data flows and data localization requirements forces countries to address how these rules might affect national measures on various issues, including cybersecurity and privacy. Trade and investment liberalization has frequently required negotiators to balance this objective with other interests, such as protecting public morals, health, or national security. The balancing involves identifying legitimate reasons for restricting trade or investment, ensuring restrictions are necessary and are not abused, and resolving disagreements through dispute settlement. If the TPP and TTIP agreements follow this approach in their e-commerce

17 "Trans-Pacific Partnership: E-Commerce and Telecommunications," *United States Trade Representative*, <https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-chapter-chapter-negotiating-6>

provisions, then they will produce new governance for digital commerce that could affect national measures on cybersecurity and privacy.

Other efforts to strengthen collective action are underway. For example, countries, companies, and intergovernmental organizations established the Global Forum on Cyber Expertise in April 2015.¹⁸ The objective is to build capabilities within countries and the private sector to engage in e-commerce governance, protect privacy, bridge the digital divide, and manage cybersecurity threats. International cooperation on protecting critical infrastructure from cyber threats and improving coordination among national computer incident response teams is also increasing.¹⁹ Although something of a patchwork, these and other efforts might become important to global political economy if they influence government policies and private sector thinking about cybersecurity.

The task ahead requires understanding we can neither reproduce the conditions under which the Internet globalized without much concern for cybersecurity nor accept the damage cyber threats and fragmented policy responses to them pose to global political economy. The next part of the story might reflect patterns familiar from history – the painstaking, uneven, and decades-long crafting of collective governance that advances economic growth and national security.

¹⁸ Global Forum on Cyber Expertise, <https://www.gccs2015.com/gfce>

¹⁹ David P. Fidler, “Cyber Norm Development and the Protection of Critical Infrastructure,” *Net Politics*, 23 July 2015, <http://blogs.cfr.org/cyber/2015/07/23/cyber-norm-development-and-the-protection-of-critical-infrastructure/>