The international political economy of the hack: A closer look at markets for cybersecurity software

Patrick Burkart & Tom McCourt

To cite this article: Patrick Burkart & Tom McCourt (2017) The international political economy of the hack: A closer look at markets for cybersecurity software, Popular Communication, 15:1, 37-54, DOI: 10.1080/15405702.2016.1269910

To link to this article: http://dx.doi.org/10.1080/15405702.2016.1269910

Published online: 11 Jan 2017.

Submit your article to this journal

Article views: 18

View related articles

View Crossmark data
The international political economy of the hack: A closer look at markets for cybersecurity software

Patrick Burkart and Tom McCourt

Texas A&M University; Fordham University

ABSTRACT
This article examines the development of hacking and cybersecurity software packages as commodities, based on an international political economy of vendors and clients operating in the interstices of international law. Offensive hacking and defensive cybersecurity tools offer new means for surveillance of critics, journalists, and human rights workers, especially in corrupt or authoritarian political systems. The article provides a case study of the Hacking Team, an international “cybersecurity” firm offering spyware and surveillance systems to government security agencies, which was itself hacked and “doxed” in 2015. The leak of documents contributes new knowledge of an international political economy for software products, which exploits the digital rights of targets and which could further undermine general Internet security.

Hacking, surveillance, and cyberwarfare

The hacker has long been a liminal figure in popular communication, alternately enabling and subverting information and communication technologies by manipulating the technical code at their core. What originated as a social and technical bonding activity among engineers at MIT and other elite universities migrated to the emergent “cyberculture” (Markoff, 2005; Turner, 2006), and then on to still looser networks of individuals engaged in subverting AT&T and other monopolistic practices of the information age (Lapsley, 2013). As with “phreaking” the phone system, so too, software hacking organized around the Internet came to symbolize a variety of social and cultural resistance—hence, its attractiveness to social and political theorists. In this regard, antecedents for hacking can be found in a number of contested technologies and applications, from the ambiguous status of amateur broadcasters prior to the Radio Act of 1912 to unauthorized low-power broadcasting preceding the 21st century. In any number of other instances, too, from John McDougall’s (Captain Midnight) 1986 hack of HBO’s satellite system, which led to the traceability of unauthorized uplinks, to the recording industry’s 1998 Secure Digital Music Initiative, in which hackers and cryptologists were invited to hack music industry copy protection schemes, hackers employ their skills to earn recognition from peers in their pursuit of exploits. While the heroic hacker remains a romantic figure in popular communication and its scholarly studies, the hacker’s social function of exploiting closed systems for popular uses faced a legal crackdown in the early 1990s. A technology transfer
from hackers to police and a growing “cybersecurity” sector followed in the dot-com boom and the 9/11 watershed, as hackers’ toolkits became adopted for protecting the interests of law enforcement and the state.

Popular communication has also communicated the risks of this technology transfer, as an elaborate and global marketplace for personally identifiable information and user profiles develops in the age of broadband Internet and smartphones (Turow, 2012). Campaigns to protect online freedom, or cyberliberties, underscore the instrumental role of popular communication in promulgating human rights and social justice issues (Murphy, 2015). For example, Pirate Parties have led popular protests against mass surveillance campaigns and directed attention to the insufficient international protections for online privacy (Andersson-Schwarz & Burkart, 2015). Since 2013, WikiLeaks has exposed the widespread use of warrantless Internet and telephone surveillance by government intelligence agencies in the United States and abroad. A growing body of academic work addresses the political, economic, social, and cultural implications of ubiquitous surveillance, including sociological studies of information technology, privacy, and surveillance (Gandy, 1993; Bauman & Lyon, 2012; Marx, 2015), and communication law and policy studies (Landau, 2013; Nissenbaum, 2004). Popular accounts range from Orwell’s seminal 1984 to recent investigative news reporting (Greenwald, 2014), and the acclaimed “Mr. Robot” television series.

This article explores the development and legal status of online surveillance technologies marketed to security and intelligence agencies under the umbrella term “lawful interception.” Lawful interception (like police wiretapping) involves capturing a target’s personally identifying information and monitoring the target’s telecommunications traffic, typically (although not always) after some kind of judicial review and authorization (i.e., warrants). While lawful interception and surveillance are by definition not illicit, the issue of “authorized access” in online surveillance is highly problematized by the nature of its global power and scope. Illicit hacking is typically defined as trespass or data theft that legally “exceeds authorized access” (Tuma, 2011). Yet given the malleable nature (or dearth) of international laws and controls, the specific terms for “authorized access” are often defined by the customers for cybersecurity software rather than through jurisprudence.

Employing a political economic perspective, we examine the production, distribution, and application of “cybersecurity” software in global markets. The key components of cybersecurity software and “spyware” include techniques for stealth operation, a channel or “attack vector” for exploiting a target through personal phones and computers, and software-based vehicles for penetrating and retrieving a target’s digital data. While cybersecurity software ostensibly is designed to test flaws in networks and enhance their security, its filial relation, spyware, offers powerful potentials for harassing journalists and political dissidents, as well as compromising the privacy of untargeted “innocent bystanders” on the Internet. Recently released documentation on the cybersecurity company The Hacking Team reveals how the global market for hacking-based surveillance software poses new and significant risks to an online environment already characterized by mass surveillance and breaches of personally identifying information.

The normalization of hacking as a means of gathering intelligence also is reflected in the private sector. Antecedents may be found in media industries; for example, in 2005, it was revealed that Sony introduced a rootkit “Trojan horse” program on music discs to
disable CD ripping (Burkart & McCourt, 2006). The spyware “phoned home” to Sony every time an affected disc was played, and provided a back door to other malicious software. NewsCorp’s News of the World voicemail hacks of victims of the 2007 London bombings, as well as journalists, politicians, and other public figures, led to jail time for a prominent NewsCorp employee. In a more mundane example from the same company, NewsCorp’s News America division settled a lawsuit and paid compensation to Floorgraphics, an advertising company whose computer network it hacked to steal business documents. In addition, corporations seeking evidence of digital piracy or online file sharing played a primary role in normalizing surveillance by Internet service providers in the United States and in Europe (Burkart & Schwarz, 2013).

Given the scarcity of publicly available research about cybersecurity tools, vendors, clients, and targets, scholarly research on these aspects of hacking often remains framed in earlier, more celebratory accounts of hacker culture and the hacker ethic (evidenced in 2600 Magazine, Mondo 2000, Wired, boingboing.net, slashdot.org, and countless other examples). Hollywood contributed mightily to hackers’ cultural capital with Wargames (1983), which is said to have informed President Ronald Reagan of cybersecurity risks to the U.S. nuclear force. Levy’s Hackers (1984) updated a tradition of literary lore celebrating the hero/inventor for the computer “wizards” at MIT, as did Bruce Sterling’s mythologizing in The Hacker Crackdown (1992). Anthropological work on hackers in general, and Anonymous in particular (e.g., Coleman, 2013), has attempted to divine a shared hacking culture, a project that has also preoccupied sociologists (Jordan & Taylor, 2004).

This article takes a systemic look at the forces reshaping the network society on the model of cybersecurity standards. Its scope is the international flow of trade in packaged and custom software developed for targeting individuals and groups with online surveillance. Software, like digital media and business services, is bought and sold internationally in markets characterized by little or no regulation or political oversight aside from intellectual property rights law. Although the European Union has developed a legal framework for the protection of personally identifiable information, and regulations governing the marketing of this information, the United States has no such system. Moreover, at the international level, industry self-regulation substitutes for potentially superior personal privacy protections that could be incorporated in treaties covering trade or arms control.

Cyberwarfare involves offensive hacks taken against targets by government militaries and their proxies, with the caveat that discerning offensive from defensive measures is problematic. In 2015, the Wall Street Journal found at least 29 countries with formal military or intelligence units dedicated to offensive hacking efforts. A NATO cyberdefense researcher has compared cyberdefenses to the nuclear arms race. Then “the acronym was MAD—mutually assured destruction—which kept everything nice and tidy. Here you have the same acronym, but it’s ‘mutually assured doubt,’ because you can never be sure what the attack will be” (Paletta, Yadron, & Valentino-Devries, 2015).

Although cyberespionage linked to Russia and China has attracted significant press attention, cybersecurity experts consider the United States to have the most advanced operations (Paletta et al., 2015). U.S. hegemony is problematized by the ways in which cyberwarfare contributes to offensive parity between large and small countries. Since cyberwarfare is based in code, it lacks the manufacturing, warehousing, and deployments costs associated with traditional weapons. Cyberattacks are relatively inexpensive and cost-effective: According to
cybersecurity firm Splunk, “The cost of cyberattacks is 1/10th to 1/100th the cost of cyber defense … This is because attack tools are freely distributed, the computing resources are stolen, and because the labor costs in state-sponsored attacks are typically low” (Williams, 2016).

The parameters of a multibillion-dollar industry—the organizations which Reporters Without Borders terms “digital mercenaries” (Kushner, 2016)—have come into focus. The WikiLeaks archives reveal an industry of firms-for-hire that sell cyber-armaments such as “zero day” exploits and coordinate targeted attacks on corporations, governments, and individuals. In particular, these firms feed exploits into marginal and at-risk political systems with corrupt or authoritarian governance. Dozens of firms compete for clients; industry leaders are the Gamma Group (owned by a shell corporation in the British Virgin Islands whose spyware is marketed through Germany), Israel’s NSO, and the Milan-based Hacking Team (Perlroth, 2016a). As of October 2015, intelligence and law enforcement agencies in at least 50 countries have purchased off-the-shelf spyware and contractor services for purposes of international and domestic surveillance (Paletta et al., 2015). Although ostensibly stateless, these cyber-mercenaries have benefitted from de facto state support and the current uncertainty of export controls designed for previous eras of conflict. With The Hacking Team (hereafter, “HT”) as a case study, we explore the financialization and militarization of hacking based products used for surveillance of collective action. In a vacuum created by a lack of formal political controls, the HT case reveals attempts of governments to transform political and economic behavior, often through questionably legal means. We find that in addition to surveilling and disrupting communication in complex networks, hacking also can alter codified legal, political, and corporate systems in ways that support the creation or degradation of information commodities.

**Hacking and critical political economy**

The consequences of hacking for the information-based commodity form are more than merely disruptive; they can also indicate profound changes to the creation of surplus value in labor. A critical political economy of communication, based in Mosco’s (1996) analytical categories of commodification, spatialization, and structuration, is particularly useful to examine hacking. Commodity chains form the basis for market creation in business services, information goods and services, media, and software (Schiller, 2014). The consolidation of personally identifiable information in databases constitutes links in these chains, which also are interwoven with vulnerabilities to trespass, theft, and disruption as they are developed and maintained (Mosco, 2015; Turow, 2012). Personal data generated as a by-product of online activities attain value by serving advertisers’ markets for personally identifiable information. The economic surplus value created by collecting, storing, and processing users’ personal data typically accrues to the media outlets or advertisers—unless there is theft or disruption, either of which can either slow or accelerate the information commodity’s reproduction.

Persistent data breaches have placed personal information at high risk; in addition, cyberespionage has become a pressing concern as the United States and other countries increasingly depend on intellectual property for economic growth. Theft of intellectual property is associated with a loss of international competitive advantage, and hence
security risk (Halbert, 2016). We propose that the market processes these risks by commodifying them in three ways. The first is through creating markets for cybersecurity tools, services, and labor. Exploits such as “zero-day” software bugs (fresh exploits that have not yet been patched) are harvested from legions of independent contractors and packaged into hacking software for sale in global markets. Cybersecurity labor is at least partly subsidized by the public sector. The U.S. National Security Agency (NSA) has provided a massive incubator for the cybersecurity industry, in which an elite professional corps of analysts—including engineers, network administrators, and enterprise software integrators—moves through a revolving door of management positions in industry and government as trusted emissaries.

Secondary markets for hacking include insurance against identity theft and hacking losses (worth at least $1.5 billion in premiums in 2015 [National Association of Insurance Commissioners [NAIC], 2016]) and ex post facto public relations campaigns by cybersecurity consultancies such as Mandiant, a subsidiary of the FireEye security firm (Perlroth, 2016b). Firms need to spend in both markets, to insure against catastrophic losses and to patch public relations after a hacking incident. In 2013, Mandiant released a report in which it claimed to have evidence linking Unit 61398 of the People’s Liberation Army in Shanghai to a global cyberespionage campaign. This campaign, “designed to steal large volumes of valuable intellectual property,” targeted nearly 150 companies from 20 economic sectors (Fidler, 2013). In addition to garnering extensive press coverage, Mandiant’s report boosted the market for hacking insurance, prompted recriminations from China, and catalyzed the Obama administration’s release of a new strategy to combat theft of U.S. trade secrets (Fidler, 2013). Cyber Security Executive Order 13636, enacted in early 2013, led to the creation of a standardized “framework” for cybersecurity developed by the National Institute of Standards and Technology (NIST) based on threat assessment, risk management, and network security. Thus, NIST helped rationalize secondary markets for hacking (in cybersecurity practices).

Tertiary markets for hacking include venture capital flows into cybersecurity companies, which have leapt from $1.1 billion in 2011 to $3.8 billion in 2015 (with 166 and 332 deals, respectively) (Acohido, 2016). Reflecting the rise in online risks owing to malicious hacking, cybersecurity has displaced mobile services in terms of investor interest. Worldwide cybersecurity spending is projected to rise from $75 billion annually in 2015 to $170 billion by 2020 (Morgan, 2016). The U.S. government alone earmarked $14 billion to cybersecurity expenses in 2016, up 10% from 2015. A newly launched exchange traded fund, the PureFunds ISE Cyber Security ETF, traded under the ticker symbol of “HACK,” adds to the froth in the market. The froth is also reflected in the dizzying values of cybermercenary firms. For example, in 2014, the United States-based investment firm Francisco Partners purchased a controlling interest in NSO Group for $120 million. Within a year, the firm sought to sell NSO for 10 times that amount (Perlroth, 2016c).

The global ownership and operations of Gamma, NSO, and HT demonstrate the spatialization of commodity chains for cyber exploits. Moreover, the “territorialization” of hacking law refers to the ongoing project of expanding U.S. jurisdiction abroad. Territorialization would require the creation of “global warrants” issued for those accused of hacking and wanted for prosecution in the United States, together with expanded authority for police hacking into targeted computers (Noglobalwarrants.org, n.d.). INTERPOL presently coordinates many antihacker campaigns internationally. And of
course, the global deregulation of telecommunications and information policies, starting with multilateral and plurilateral agreements such as the World Trade Organization, World Intellectual Property Organization, and the European Union Copyright Directive, has preceded territorialization of hacking law and created new demands for its implementation.

The growth of the outsourced surveillance industry

In 2014, the private online surveillance industry generated more than $5 billion in profits (Sankin, 2015). By 2021, the cybersecurity market is estimated to be worth over $202 billion, particularly due to security breaches targeting corporations, the developing Internet of Things, and the growth of cloud-based business applications (“Cyber security markets,” 2015). The U.S. government alone earmarked $14 billion to cybersecurity expenses in 2016, up 10% from 2015: “The Government also allocated US $582 million to its Continuous Diagnostics and Mitigation (CDM) program, which emphasizes management of federal systems inventories, including determining who is on the network and their purpose for being there” (Mergent, 2016, p. 14).

Cybersecurity markets developed before the year 2000, as IBM, Microsoft, Cisco, and other information technology companies began marketing services to outside firms. By 1998, accounting firms such as Price Waterhouse LLP, Coopers & Lybrand LLP, and Ernst & Young LLP offered “swat teams” to clients; between the end of 1996 and March 1998, Price Waterhouse alone tripled its cyber security business (DiDio, 1998). In 1998, Microsoft established an internal hacking team (the 24–7 Security Problem Response Team) and formed partnerships with a host of private companies and public agencies, such as CERT at Carnegie Mellon University and CIAC at the U.S. Department of Energy (Burns, 1998). At present, the leading firms include Intel Security, Symantec Corporation, Hewlett Packard, IBM, Cisco Systems, Rapid7, EMC RSA, FireEye, Inc. (all based in the U.S.), Trend Micro, Inc. (Japan), and Sophos Ltd. (UK; MarketsandMarkets, n.d.). University programs and “capture-the-flag” hacking contests also serve as venues for cybersecurity research and development. In October 2014, the Washington Post detailed “hacking schools” operating at the University of Tulsa and at Carnegie Mellon in Pittsburgh. The 2014 DefCon hacking conference in Las Vegas, NV, featured “a ‘capture-the-flag’ competition in which 20 teams attempted to breach each other’s computers” (Nakashima & Soltani, 2014).

The domestic cybersecurity industry is based on a revolving door between government, academics, and industry established before the 2001 watershed of 9/11. The National Security Agency (NSA) has long served as an incubator for startups in computer and network security. For example, Trusted Information Systems, Inc. (TIS), a Glenwood, MD, based computer-security firm, was founded in 1983 by a former NSA and Defense Department researcher (Chandrasekaran, 1998). The company focused on four primary areas: firewalls, antivirus software, VPNs (virtual private networks), and intrusion detection software against “insider” hacks. TIS’s success led to its purchase by Santa Clara, CA, based Network Associates, Inc., for $307 million in 1998 (McIntosh, 2000). Also, former CIA director R. James Woolsey and many NSA veterans have sat on the board of directors of Invicta Networks, founded by Soviet defector Victor Sheymov (Risen, 2000). The post-9/11 “Gold Rush” in computer and network security accelerated the revolving door between
government agencies such as GCHQ/NSA and industry, and created some ancillary services. For example, General Keith Alexander, former U.S. Cyber Command and NSA head, “now attracts vast seven-figure consulting fees for his IronNet Cybersecurity firm. This after Alexander left the NSA under a cloud ... over [Edward] Snowden’s revelations of NSA bulk surveillance and warrantless wiretapping” (Moroney, 2014).

Just as traditional arms manufacturers claim to provide “defensive” capabilities, these firms are primarily engaged in developing offensive measures:

None of their software will help clients avoid cyberattacks, tighten up their internal networks, or patch flaws in their software. [Their] main business is offensive hacking ... [selling] software to law enforcement and national security agencies around the world, letting them hack into targets’ computers and mobile devices, install backdoors, and monitor them with ease. (Hern, 2015b)

Defense double-speak pervades cybersecurity studies.

Cyberwarfare relies on “dual-use” tools with both military and civilian applications (as, e.g., nuclear materials may be used for bombs and as a source of energy). Software that targets external threats can also be used to track domestic activity. While state agencies rationalize the application of these dual-use tools in the name of counter-terrorism or countering criminal activity, it appears that the majority of these applications are used for domestic surveillance and political purposes, underscored by the burgeoning international marketplace of arms bazaars for “lawful interception.” Worldwide sales of interception technology are estimated to reach $1.3 billion by 2019 (Risen, 2015). These technologies are showcased in global trade shows featuring large corporate subsidiaries; independent firms that sell spyware and malware to state security and law enforcement entities; and third parties, akin to traditional gunrunners, that link independent firms to states and police. The Intelligence Support Systems (ISS) World Americas conference, nicknamed the “Wiretappers Ball,” is one of several conferences held around the world each year organized by TeleStrategies, a Virginia-based firm (Risen, 2015). These events are closed to media and members of the public. A Washington, DC-based surveillance and privacy expert told the Guardian about concerns raised by these private markets:

When there are five or six conferences held in closed locations every year, where telecommunications companies, surveillance companies and government ministers meet in secret to cut deals, buy equipment, and discuss the latest methods to intercept their citizens’ communications—that I think meets the level of concern ... They say that they are doing it with the best of intentions. And they say that they are doing it in a way that they have checks and balances and controls to make sure that these technologies are not being abused. But decades of history show that surveillance powers are abused—usually for political purposes. (as quoted in Gallagher, 2011, para. 7)

Concerns about abusive surveillance practices have been widespread for decades in authoritarian political systems, especially those with unstable or divided political support. At the end of the Obama era, with eroded safeguards against politically motivated (including those algorithmically generated), warrantless mass surveillance, and with strengthened powers delegated to the executive branch, such concerns have been amplified in the United States and other Western countries as well (Greenwald, 2016).
The Hacking Team

Hailed as “the Blackwater of surveillance,” the Milan, Italy-based HT has been a fixture at ISS shows (Kushner, 2016). In 2001, Italian programmers Alberto Ornaghi and Marco Valleri wrote Ettercap, a free open-source program for detecting passwords, eavesdropping, and remotely manipulating target computers. In 2003, Ornaghi and Valleri added David Vincenzetti as chief executive officer (CEO) and formally incorporated as HT. Under Vincenzetti’s direction, HT focused on developing malware and other offensive capabilities, releasing Remote Control System (RCS, or Da Vinci) in 2003. Promotional literature touted RCS as enabling authorities to break into hardware such as computers and smartphones and control microphones and webcams to monitor subjects through surreptitious recordings and screen captures, as well as allowing authorities to remotely upload files and retrieve information such as e-mails, passwords, and documents from targets.

An RCS program could scale from one to hundreds of thousands of targets. RCS could be physically installed via a USB stick (if authorities could directly access the computer), or remotely through e-mail attachments or phishing scams, as well as “network injectors” (physical devices housed with Internet service providers that enable authorities to intercept ordinary Web traffic, such as streaming video, and replace it with infectious code). HT claimed that RCS could also emulate or spoof access points, pretending to be a free WiFi hotspot to which targets had connected previously (Currier & Marquis-Boire, 2014). RCS functions also could be pushed onto phones via telephone companies and allowed tracking users via global positioning systems (GPS). By 2013, HT counted 35 employees, with offices in Milan, Italy; Annapolis, MD; and Singapore. The 2015 revenues were $17.5 million; HT’s clients have paid between $50,000 and $2 million annually for RCS depending on the number of targets and platforms (Kushner, 2016).

The commodity chain for custom-configured spyware spans international labor and currency markets and free-trade regimes. However, spyware production is complex and fraught with uncertainties. Continual updates are required to maintain effectiveness as holes in code are discovered and patched. Spyware vendors frequently use a subscription business model, as this allows buyers to minimize risk by parceling out payments over time and terminating these payments if a given vulnerability is patched before the subscription expires (Tsyrklevich, 2015). As with other markets for media, subscriptions also allow the company to book revenues up front and potentially retain customers after an initial purchase. Comparing the reliability and projected longevity of exploits also is difficult. Depending on the quality, freshness, scarcity, and breadth of application, prices for exploits may range from the low thousands to over a million dollars: The greater the platform’s sophistication (such as Apple’s iPhone), the higher is the price of the exploit.

The exchange value of zero-day exploits, based in their labor-intensive production and scarcity, is further enhanced by secrecy. HT and other cyber mercenaries rely extensively on outside vendors for zero-day exploits; HT began working with vendors in 2009 as the company was transforming from an information security consultancy to a surveillance firm. Although HT sought to develop in-house talent and establish new contacts with developers toward this goal, this was met with mixed success. Since many established vendors and brokers preferred to sell exclusively to governments, rather than private
companies, HT’s suppliers were often small or marginal concerns, and obtaining exclusivity rights was problematic (WikiLeaks, 2015).

HT was first linked directly to attacks on dissidents in 2012. Hisham Almiraat was editor and co-founder of Mamfakinch, a Moroccan pro-democracy website created during the Arab Spring. On July 13, 2012, Almiraat and his colleagues received an e-mail with “Denunciation” in the subject line. “Please do not mention my name or anything. I do not want any trouble,” wrote the sender. A website link directed them to a document labeled “Scandal,” which, once downloaded, was blank. Morgan Marquis-Boire, who worked in Google security and volunteered for the Citizen Lab research group based at the University of Toronto’s Munk School of Global Affairs, examined the e-mail and found that anyone who opened it had been infected with spyware originating from an IP address linked to Morocco’s Supreme Council of National Defense, which operated the country’s security agencies. A few lines of source code unwittingly left in the Scandal document led directly to HT (Kushner, 2016).

In March 2013, Reporters Without Borders included HT on its annual Corporate Enemies of the Internet list, and warned that online surveillance posed “a growing danger for journalists, bloggers, citizen-journalists, and human rights defenders” (Kushner, 2016). The list also included Gamma (whose FinFisher system was sold to Bahrain, Turkmenistan, Ethiopia, and South Africa, among others) and BlueCoat Systems, a United States-based firm that has sold monitoring systems to Iran, Syria, and Sudan. Claiming that “one person’s activist is another person’s terrorist” (Brewster, 2013), HT spokesperson Eric Rabe countered that “the software we provide is essential for law enforcement and for the safety of all in an age when terrorists, drug dealers and sex traffickers and other criminals routinely use the Internet and mobile communications to carry out their crimes” (Plus Media Solutions, 2014).

As alarms sounded over these revelations, and concerns about the proliferation of its software grew, HT claimed that the company’s checks and balances included an external board of lawyers and engineers who vetted potential clients, with the power to “veto any sale” (Gilbert, 2013). HT has also stated that its license prohibited users from passing along technology to third parties (although how this was enforced is unclear, aside from claims that its “audit tool” could trace how software is used). Information technology (IT) security author and cryptographer Bruce Schneier claimed, “They just need plausible deniability because … morally it’s like selling [electro]shock batons to South Africa in the 1960s” (Worrall, 2013). Although HT claimed it took extensive precautions to limit potential for abuse, in late 2013 Citizen Lab reported that clients in the United Arab Emirates, Bahrain, Morocco, Ethiopia, Vietnam, and Turkmenistan were using HT malware to target and harass political activists and dissidents, human rights workers, and journalists. HT declined to confirm or deny the identities of its licensees on the grounds that such “information could jeopardize legitimate investigations” (Timberg, 2014).

The Hacking Team hacked

On August 6, 2014, hacktivist Phineas Fisher (a play on Gamma’s FinFisher spyware suite) leaked 40 GB of marketing and technical information from HT rival Gamma online. Eleven months later, on July 5, 2015, Fisher hijacked HT’s Twitter account. He changed the account’s name to the Hacked Team, altered the bio to “Developing ineffective, easy-to
offensive technology to compromise the operations of the worldwide law enforcement and intelligence communities,” and posted a message which read “Since we have nothing to hide, we’re publishing all our emails, files, and source code” (Goodin, 2015). A BitTorrent link was included, which allowed access to more than 400 gigabytes of the company’s most sensitive data, including passwords, internal e-mails, exchanges with clients, and 80% of the company’s source code, including the zero-day exploits that were in its arsenal (Lemos, 2015b). Fisher apparently gained access to an HT engineer’s computer while it was logged into the network. The engineer’s password was Passw0rd (Greene, 2015).

WikiLeaks created a searchable archive of HT e-mails culled from the online data dump, including a spreadsheet that listed HT’s active and inactive clients at the end of 2014. In addition to the countries listed by Citizen Lab, the spreadsheet revealed that HT clients also included law enforcement and security agencies in Egypt, Nigeria, Oman, Lebanon, Bahrain, India, Mexico, Ecuador, Thailand, South Korea, Russia, Italy, Hungary, and Switzerland. Mexico provided the largest revenues to HT, followed by Italy and Morocco (Hern, 2015b). U.S. clients included the Florida Metropolitan Bureau of Investigation, which paid HT more than $400,000 (Smith, 2015); the Drug Enforcement Administration (DEA), which paid HT $2.4 million for RCS in August 2012 in order to spy on 17 “foreign-based drug traffickers and money launderers” (Kushner, 2016); and the FBI, which paid HT more than $773,000 since 2011 (Goodin, 2015).

Although the FBI had developed malware in 2001 known as Magic Lantern, which could take over a computer and log its user’s keystrokes and bypass encryption (Currier & Marquis-Boire, 2014), the agency likely was hedging its bets by monitoring technological developments and potential competitors/adversaries. So was Russia. Exfiltrated documents revealed that HT sold RCS to KVANT, a Russian-owned military research and development firm that works with Russia’s secret police, the FSB. KVANT established a relationship with FSB through NICE, an Israeli company that specialized in surveillance and data security and acted as a reseller for HT’s tools (Fox-Brewster, 2015). The WikiLeaks archive also indicated extensive negotiations with third-party partners in India and Pakistan. It also revealed that HT specifically targeted Bitcoin and other cryptocurrencies to allow governments to exploit Bitcoin anonymity protections and “follow the money” trails (Lemos, 2015a).

The posted documents revealed that, contrary to the company’s claims, HT undertook only the most pro forma and superficial vetting of clients and contractors, and cultivated extensive negotiations with police and state security agencies accused of human rights violations. Along with Russia’s KVANT, leaked internal documents listed Sudan’s National Intelligence Security Service as “not officially supported” by HT, rather than as having “active” or “expired” status as a client (Hern, 2015a). Although HT denied it had ever done business with Sudan, which was under a UN arms embargo, a June 2012 invoice for €480,000 to the Sudanese security service was posted (Auchard & Menn, 2015). HT claimed that its programs were sold in Sudan before dual use technologies were regulated. “If one sells sandwiches to Sudan, he is not subject, as far as my knowledge goes, to the law. HT should be treated like a sandwich vendor,” the firm’s legal counsel argued (Kushner, 2016).

After initially blaming an unspecified government or governments for the hack of HT, Vincenzetti speculated that it could have been an “inside job” by former employees,
although Italian authorities brought forward no charges (Gibbs, 2015). According to Vincenzetti, HT lost 20% of its customers following the leak, including its U.S. clients, but the company still reported $14 million in revenue for 2015 (Kushner, 2016). HT rewrote its software from scratch for 3 months after the breach, resulting in what Vincenzetti trumpeted as a “much better” product (Kushner, 2016). However, Italy implemented the Wassenaar Arrangement, a multinational pact that governs the exports of dual-use goods, on January 1, 2015. The arrangement, created in 1996, had been amended to include surveillance software, which meant the Italian government would now vet HT’s clients. In early April 2016, the Italian Ministry of Economic Development (MISE) revoked HT’s global license, with subsequent licenses for clients outside of Europe to be obtained on a case-by-case basis. HT still has approvals for all countries within the European Union (EU) (Fox-Brewster, 2016).

Global surveillance continues unabated through other vendors such as Gamma and NSO (Perlroth, 2016c). On August 11, 2016, United Arab Emirates (UAE) activist Ahmed Mansoor received text messages on his iPhone promising “new secrets” about detainees tortured in UAE jails if he clicked on an included link. Instead, Mansoor sent the messages to Citizen Lab researchers. Citizen Lab recognized the links as belonging to an exploit infrastructure connected to the Israeli NSO Group. Their report claimed:

The high cost of iPhone zero-days, the apparent use of NSO Group’s government-exclusive Pegasus product, and prior known targeting of Mansoor by the UAE government provide indicators that point to the UAE government as the likely operator behind the targeting. (Marczak & Scott-Railton, 2016, para. 6)

Mansoor had won the spyware trifecta: In addition to harassment by NSO, he was targeted by HT’s RCS spyware in 2012 and FinFisher’s FinSpy spyware in 2011 (Marczak & Scott-Railton, 2016). On behalf of victims of FinFisher software, Privacy International and Bytes For All filed unlawful surveillance complaints and privacy lawsuits against the Bahraini and Pakistani governments, respectively (Citizenlab, 2015). The Electronic Frontier Foundation brought suit in the United States against HT on behalf of an Ethiopian opposition party member who had been targeted with spyware by the Ethiopian government in 2011 (Goyett, 2015).

The market for software exploits indicates that prospects for compensation from the cybersecurity industry exceed those from the software vendors themselves:

Companies in the market, such as Acton [and] Netragard Inc., pay bug hunters more for the information than the makers of the flawed software themselves. Netragard CEO Adriel Desautels says that while the software industry might pay a few thousand dollars for vulnerabilities to patch systems and better protect customers, his company sometimes pays $100,000 or more for an exploit of an unknown flaw. (Silver, 2012)

Until recently, Yahoo paid researchers who discovered vulnerabilities with an online voucher for a T-shirt, while Apple offered no payment at all (despite revenues of $182 billion in 2014; Batey, 2015). Beginning in 2008, an exploit in Apple’s iTunes enabled third parties to install unauthorized programs in online updates of the program. At security trade shows, a Gamma demo showed prospective clients how to install FinFisher on users’ computers using iTunes’ update procedures. Remarkably, Apple did not patch the flaw until November 2011 (Williams, 2011). Disclosing zero-day vulnerabilities to cybersecurity enterprises, rather than to the originating software vendors,
encourages these organizations to stockpile them against potential adversaries instead of reporting them as bugs. However, the longer the zero-day exists, the more likely it is to escape into “the wild,” leaving the public exposed and the network as a whole devalued by increased risk.

Hackers also may be given security clearances to enable firms to perform vulnerability assessments for government agencies. Computer Sciences Corporation (CSC) “emphasizes that CSC doesn’t hire reformers—cyber-outlaws who crossed the law in the past but who’ve had a conversion. ‘Some of those hackers have turned totally ethical, but there have been some cases where they haven’t,’” according to a spokesman (Wingfield, 2002). The University of Tulsa’s “hacking school” has claimed that students are screened for security clearances and must “promise” to work for the National Security Agency, Central Intelligence Agency, or another government agency upon graduation (Nakashima & Soltani, 2014). The ironies abound in trusting hackers to defend “trusted” systems.

**Cyberattacks and international law**

Cyberattacks defy easy classification and codification. They may include espionage, terrorism, theft, vandalism, or protest; the lines between categories may be blurred, compounded by the difficulty of ascertaining perpetrators and motives. While criminal hacks may seek a quick financial return, state-based attacks may intend to collect strategic or technical information that later can be employed for disruptive purposes. Yet both criminal and state hackers may use similar means and methods, making the perpetrators harder to differentiate. Reflecting the growing alliance of state and corporate actors, methods used by states may transfer formally to private firms. Also, attacks are not necessarily waged between individual entities (such as single nation vs. single nation). These ambiguities and undefined boundaries readily lead to a “fog of war” scenario in which agency appears to be everywhere and nowhere.

The vagaries of delimiting cybersecurity in offensive, defensive, and hybridized terms carries over to the legal realm, where an overly broad codification of “cybercrimes” entraps activists and tinkerers, while seeming to exclude exporters and purchasers of cyberweapons. The vaguely defined and shifting categories of actors and actions, combined with the dualism of defensive and offensive measures, have led to a series of overlapping initiatives that exacerbate the challenges to coordinating diplomatic, economic, or military responses to cyberattacks. At the international level, the Council of Europe’s Convention on Cybercrime provides a legal regime for its 47 signatory states (which do not include China, Russia, or Brazil). Although it lacks a political mandate, the Convention on Cybercrime requires signatories to punish offenders “by effective, proportionate and dissuasive sanctions, which include deprivation of liberty” (Council of Europe, 2001, Article 3, Section 1). The U.S. Senate ratified the Convention on Cybercrime in 2006, adopting European standards that criminalized illegal access and interception, data and system interference, misuse of devices, computer-related forgery and fraud, offenses related to child pornography, infringement of copyright and related rights, and aiding and abetting these offenses. The United States also committed to extradition and mutual assistance in pursuing cases, including intercepting and sharing traffic and content data from service providers in real time.
In 2011, the United Kingdom promulgated the UK Cyber Security Strategy for countermeasures, and “has developed additional capacities to effectively counter cyberattacks” (Lee & Lim, 2016, p. 860). In 2014, NATO declared that cyberattacks on one or all members should be considered an attack on all allies (Lee & Lim, 2016, p. 860). The EU is currently implementing the Directive on Network and Information Security to help establish cybersecurity systems on the model of the 2013 Cybersecurity Strategy of the European Union. The EU and NATO have “discussed the potential for cooperation in response to Russia’s hybrid warfare, which includes cyberattacks,” and three executive orders by President Obama have proposed public–private information sharing and “severe punishment for hackers and their accomplices” in cyberattacks (Lee & Lim, 2016, p. 860).

Notwithstanding these measures, the commodity chain for hacking products and services has evaded comprehensive, or even substantial, regulation to date. The Wassenaar Agreement, mentioned earlier, is considered to be the most likely vehicle for reining in abuses by cybersecurity vendors. The United States and 40 other countries (although neither China nor Iran) are signatories. In 2013, the Wassenaar Agreement was amended to include controls for surveillance software of the sort sold by HT, Gamma, and other vendors. Yet the Wassenaar Agreement remains riddled with holes. In the EU, for example, export licenses are issued on a country-by-country basis, rather than by a centralized clearinghouse, with resultant lax enforcement. In Britain, the Export Control Organisation (ECO) licenses exports of weapons—but these licenses must be applied for. As one observer noted, “Virtual weapons don’t sit in packing crates ready to be examined by customs officers; they may be being developed and sold globally without the ECO ever knowing they exist” (Batey, 2011). Countries are hesitant to regulate software they also utilize, or to penalize the companies that create it within their borders. Within the EU market, sales of “cybersecurity” software and services bypass national tariffs, taxation, and trade accounting, especially among World Trade Organization (WTO)/UN World Intellectual Property Organization (WIPO) signatories and other liberalized trade relationships.

In May 2015, the U. S. Commerce Department issued a proposal, modeled on Wassenaar, which would have added new licensing requirements to export “intrusion software.” In response, U.S. firms formed the Coalition for Responsible Cybersecurity, a single-issue group dedicated to torpedoing the Commerce Department proposal. Rep. Jim Langevin (D-RI), who co-chaired the Congressional Cybersecurity Caucus, represented its interests in a letter that stated, “The proposed rule has a number of flaws that could detrimentally affect our national security … This could have a chilling effect on research, slowing the disclosure of vulnerabilities and impairing our nation’s cybersecurity” (Bennett, 2015). Opponents criticized the licensing requirement for zero-day exploits, regardless of purpose or final destination: “Network-testing equipment sent to England would face the same potentially onerous scrutiny as spyware sent to Syria” (Uchill, 2015).

The crux of this debate turns on the profitable maintenance of a steady supply of hacker labor and artifice required to integrate and package surveillance tools within “turnkey” suites of software. The Commerce Department’s proposal would have made it more difficult to sell a wide range of Web-related equipment and software overseas. Netragard claimed the bill would “completely [destroy] vulnerability research” (Bennett, 2015); the Commerce Department responded, “Vulnerability research is not controlled nor would the technology related to choosing, finding, targeting, studying and testing a vulnerability
be controlled.” A representative for the Commerce Department’s Bureau of Industry and Security stated that regulators only want to control “the development, testing, evaluating and productizing of an exploit or intrusion software, or of course the development of zero-day exploits for sale” (Bennett, 2015). However, it is virtually impossible to discriminate between companies developing and testing software that probes vulnerabilities and those in efforts to develop zero-day exploits and intrusion software. As the Electronic Frontier Foundation writes, “The only difference between an academic proof of concept and a zero-day for sale is the … price tag” (Bennett, 2015).

**Conclusion**

The political economic model of commodification, spatialization, and structuration holds explanatory power for the normalization of hacking as a state and corporate practice. First, the cybersecurity market has fueled a boom in products and services built on hacking. Hacking episodes may either slow or accelerate the circulation of an information commodity and its underlying “layers” of data and knowledge work, especially when the commodity inheres in longer commodity chains with interconnected markets for media, information, and services (Schiller, 2014). These chains form the basis for creating markets in business services, information goods and services, media, and software; they may very well hold the informational “keys to the kingdom” for elites who utilize the revolving door between government and industry for access. As these chains are gathered and braided, vulnerabilities to disruption and cyber theft become interwoven among them—yet these vulnerabilities in turn may work to the benefit of the markets. Exploitation risks for databases full of personally identifying information have developed into significant, global, and real-time markets for cybersecurity defenses against hacking.

Secondary markets include the offerings of HT and other firms at the state level, as well as cybersecurity insurance policies and post-hack public relations for corporate and personal clients. The “HACK” exchange traded fund represents a tertiary market for hacking’s commodification, and is a fully fledged “cybernetic commodity” (Mosco, 1989). In sum, the international political economy of primary, secondary, and tertiary markets for commercial hacking products is bounded by the logic of exchange and strategic-rational action. It is shaped by the commodification of hacking in cybersecurity markets and the subsidization of these markets by the NSA, and governed by international frameworks (however underdeveloped they may be at the present time).

With regard to spatialization, international linkages among technology, capital, and labor intensify hacking’s commodification. Territorialization, based in the global deregulation of telecommunications and information policies through multilateral and plurilateral trade agreements, requires the creation of “global warrants” for those accused of hacking and wanted for prosecution, together with expanded authority for police hacking into targeted computers (Noglobalwarrants.org, n.d.). In terms of structuration, the markets for “security” require a sociotechnical system of universal surveillance that has been partly mapped by Snowden, Greenwald, Schneirer, CitizenLab/University of Toronto, and others. In its geographical expansiveness, intelligence and police surveillance systems have grown to meet the needs of governments pursuing advantages for themselves and their clients through exploits, espionage, and information warfare. The profiling processes that are the product of the “panoptic sort” (Gandy, 1993) in the end contribute
to a restructuration of social classes based on “suspicious” but familiar characteristics pertaining to religion, race, country of origin, politics, and employment.

The rise of the information state corresponds to “with the era of neoliberalisation, the political economic model that is currently in crisis” (Bates, 2014, p. 388; Schiller, 2014). The “fog of war” in cybersecurity descends in large part from a lack of transparency, accountability, and checks and balances. Yet measures to address these issues are highly problematic in an age of virtual systems and compounded by the very nature of dual-use technologies. While these technologies are rationalized in the name of countering terrorism and criminal activity, their implementation more often than not is at least partly dedicated to surveillance of private citizens, journalists, and political opponents of incumbent regimes. They have become so invasive that oversight is nearly impossible, and attempts at regulation could very well drive the market for such products deeper underground. Under a partially privatized security state, the “intelligence community” is a priestly caste replenished by the revolving door between government, academics, and industry and supported by police and intelligence agencies, mercenaries, and other state proxies. These confused social roles, rules, and resources have exponentially increased markets for instruments to manage risk in online networks—at the expense of civil liberties and the security and integrity of the Internet.

ORCID
Patrick Burkart @ http://orcid.org/0000-0001-5024-6963

References


Goyett, J. (2015, July 8). For this group of Ethiopian journalists, the Hacking Team revelations are personal. PRI.org. Retrieved from http://www.pri.org/stories/2015/07-08/these-ethiopian-journalists-exile-hacking-team-revelations-are-personal


