The AMERICAN INTEREST
https://www.the-american-interest.com/2017/05/22/piracy-on-the-cyber-seas/

Published on: May 22, 2017
STATES UNDER STRESS

Piracy on the Cyber Seas

ADAM GARFINKLE

How the disintermediation and hyperconnectivity afforded by the cyber revolution threaten the order of the commons, and thus the Westphalian state system itself.

The massive ransomware attack of May 12 made news for a few days and then, like Andy Warhol's 15-minutes of fame, dropped pretty much out of the mainstream press ambit. This is understandable, perhaps, since this episode of a ransomware attack was noteworthy for only two reasons: It was much grander than all its precursors, which go back at least to 2012; and it made use for the first time of NSA tools purloined last summer by a shadowy group called, appropriately enough, the Shadow Brokers.

Otherwise, most would-be victims refused to pay, and Microsoft gave out free patches to spread protection and protect its own bottom line. The damage seems to have been fairly limited in part because the perpetrators failed to set up a payment flow in a clean and timely manner, and because almost no bank will convert Bitcoin to cash. Besides, much of the damage seems to have occurred in China, where more vulnerable bootlegged software is ubiquitous: serves the thieving bastards right.

So, all's fairly well that ends fairly well? Not so fast. The bad guys are still at large, whether they are common criminals or virtually armed anarchists seeking to tank the "system"—and we don't yet know which. Maybe both. The Shadow Brokers are probably Russia-backed goons one or two or three degrees of separation removed from Russian intelligence, but they seem not to have been running the extortion attempt. As soon as the Shadow Brokers dumped the NSA tools, this sort of thing was inevitable. Yet as amateurish as the second-echelon hackers seem to have been—whether plain criminality of politically inflected criminality was the motive—that doesn't mean they'll be easy to catch or deter, or that other hackers won't try similar things. So as a generic problem, this is not even close to being over.

Distinguishing simple criminal from political criminal motives is not easy, and never has been—but it is important. And the reason is that during its short period of fame, no one identified the ransomware event in its proper historical category. Many observers referred to "extortion" and others less specifically to "theft." Those terms are not wrong but they miss the essence: This was an act of piracy, *piracy on the cyberseas*.

To miss this obvious insight, one has to be asking inadequate questions. As the late and very great British anthropologist Mary Douglas once wrote, "Information is simply not going to rub off on someone who is never going to make use of it."[1] What use should we be making of the ransomware incident? What questions should it pose?

Some of the answers come clear if we recall the definition and some of the history of piracy. In his 2009 book, *The Enemy of All: Piracy and the Law of Nations,* Daniel Heller-Roazen of Princeton University provides as good a definition as we need. Piracy, he reminds us, emerges from a conjunction of four conditions: It occurs in a region beyond territorial jurisdiction; its agents are not identified with an established state; it obfuscates or collapses the distinction between criminal and political categories; and it transforms the concept of war by ignoring all its framework assumptions and explicit rules (to the extent there are any).

The pirate, as all international legal experts know, is the original enemy of humankind: *hostis humani generis*. The concept is usually attributed to Cicero, who famously remarked that, while there are certain enemies with whom one may negotiate and with whom, circumstances permitting, one may establish a truce, there are others with whom treaties are in vain and war remains incessant. The Latin phrase, however, seems to be the early modern coinage of the nearly-as-famous English jurist Edward Coke (1552-1634).

No matter. The definition in modern times has been extended from pirates to terrorists—and, by some, to torturers as well. But again, as was the case with pirates back in the day (or to Somali pirates around the Horn of Africa much more recently), disentangling those who are irreconcilably but simply criminal from those with a political axe to grind isn't easy. In the 17th century, for example, some people's pirates were other people's privateers—ask some Spanish and English ghosts if you don't believe me, or just read up on Sir Francis Drake. And today, some people's terrorists are said (wrongly) to be other people's freedom fighters. And yes, now some people's malware criminals are said to be anarchist heroes trying to destroy global capitalism, allegedly a sinister system perpetrating massive inequality and other forms of "structural violence."

The point in all cases is that the "pirate" rejects the principle of the system of norms that enables law and order to serve all. That is why, as Heller-Roazen explains it, the pirate in legal and political thought from the ancient to the medieval, modern, and contemporary periods embodies the idea of a universal foe—a legal and political person of exception, neither clearly criminal nor enemy, who inhabits an extra-territorial region—against whom states may wage extraordinary battles, policing politics and justifying military measures in the name of the general welfare and security of the commons.

Heller-Roazen argues that the paradigm of piracy remains in force. He clearly has terrorism in mind, defined as "indiscriminate aggression" committed "against humanity." When I invited him to extend his thinking to encompass ransomware culprits, he acknowledged the applicability but begged off the task, claiming he knew too little about the software. (I answered that he was maybe missing the point, but it did no good; so here I'm trying to do what he probably could do better. Again, no matter.)

So why exactly was the May 12 piratical attack so important, so much more deserving that the "15 minutes" of mainstream press coverage it has gotten? Because it illuminates the four conditions of piracy the attack fit so well. It shows, simply put, how the massive disintermediation and hyperconnectivity afforded by the cybernetic revolution threaten the order of the commons we have—in other words, how it threatens the *raison d'être* of the Westphalian state and state system with it.

Before getting to the four "fitted" conditions of the May 12 attack, allow please a very short description in the context of both disintermediation and hyperconnectivity, *as seen together*.

Disintermediation means the dismantling of buffering structures between individuals and between individuals and institutions, including governments. Relatively benign examples include AirBnB, Uber, ATMs, “smart” gas pumping machines, online travel sites, and we can obviously go on and on. But hackers-*cum*-pirates, too, can strip out all the intermediate structures that used to separate an individual’s or a company’s proprietary information sets from malicious agents wishing to steal, destroy, distort, or fake-and-transmit that information for any of several nefarious purposes. It is also why, in an age of electronic medical records, laws have had to be passed to protect those records from theft and manipulation, it’s why identity theft is a growing criminal problem, and again we could go on.

If disintermediation allows bad guys to surgically target victims as never before, from anywhere on the planet, hyperconnectivity enables them to multiply their targets simultaneously by many orders of magnitude. If there are something like 700 million iPhones on the planet now—never mind other brands, laptops, or personal computers—and if any iPhone can transact with any other smartphone, that yields about 2.45 x 10^{17} potential connections. As ought to be obvious, numbers like these mean that a ransomware attack that exploits a flaw in iPhone software can spread very widely, very quickly, to hundreds of millions of smartphone users. And we are likely just at the beginning of a process whereby such numbers will not only be achieved but surpassed. If cyberpirates collect even very small ransoms from just 1 percent of connected victims, that’s still an enormous amount of potential loot.

Condition 1: Back in the days of Sir Francis Drake and Blackbeard, the high seas were effectively beyond territorial jurisdiction, meaning the jurisdiction of early-modern states. By the 1970s, so was outer space beyond the effective jurisdiction of nearly all states. Today, so is cyberspace. The problem is that, as far as everyday human transactions are concerned—commercial, cultural, and others—we nations and peoples of the world are coming to depend on cyberspace as a commons far more than our forbears did on space or even the high seas. So screwing around with the use of that commons, whether for criminal or political purposes, is very tempting. Too tempting, because getting caught is still improbable because of jurisdictional friction and punishments, if caught, are not draconian enough to deter opportunists.

Condition 2: As for agents being beyond identification with a territorial state, that is a status easier than ever to achieve. Yes, nearly everyone is a national of some UN member, so in legal theory the question of jurisdiction is not manifestly more complex than it was three hundred years ago. But hyperconnectivity enables the creation of neo-tribes based on affinity like no time in the past. It is easier to be a non-national citizen of the world today than ever. It is easier to be an anarchist, therefore, than ever, and to get away with anarchist sabotage not by assassinating world leaders—as was so popular a century or so ago—but by assassinating the operating system on which all national leaders and corporate managers increasingly depend.

Condition 3: As for obfuscating or causing to collapse the distinction between the criminal and the political, ransomware attackers illustrate a piling-on to the twin attack on the state ably described in the pages of *The American Interest* by Nils Gilman. In his 2014 essay, "The Twin Insurgency," he shows how criminals and plutocrats unwittingly (for the most part) reinforce each other's attack on the state, each creating forms of porosity the other can walk right through. We may now imagine a triple insurgency, adding modern political pirates to the mix. If it turns out, as I suspect is likely, that many would-be piratical hackers have a political agenda akin to the other well-known transparency saints of our time—Assange, Snowden, Manning—then we will see the concept of *hostis humani generis* come alive yet again before our very eyes.

Condition 4: At a time of massive disintermediation and hyperconnectivity, we are still trying to work out the implications not just for war as we have known it, but also for related concepts like security, deterrence, and even peace. The basic issue is the new problematics of the platform, both political and operational.

Since at least 1648, the unit of measure has been the state, the idea being that if the state could defend itself it could also defend the people within it. That has never been completely the case, but it was close enough for government work when the only borders were horizontal ones. Then aircraft, starting in 1911, could be agents of death for soldiers and civilians alike even if land borders remained secure. Space operations, in theory at least, created a third dimension of vulnerability—let's call it orbital/circular in addition to horizontal and vertical—in the latter part of the 20th century. And now, in the 21st, we are witness to a fourth dimension, virtual borders in cyberspace.

As each dimension got added over time, the efficacy of the state to manage the implements and environment of war declined, radically so in this new four-dimensional condition. States still remain arguably the most important actors, but the share of variance they cannot effectively control is rising before the twinned tides of disintermediation and hyperconnectivity. That means that the rules of protocol they propound mean less and less as time passes, for increasingly powerful agents not party to membership are proliferating. That represents a conceptual change in war (and related core concepts), especially at a time when private multinational (or at any rate psychologically de-nationalized) corporations are spending a lot more research and development dollars than are governments. What if some private corporation perfects the use of nanotech distributed systems to defend and/or attack human populations before any state does? Will we find ourselves in a yet unwritten chapter of *Diamond Age*? We frankly have no idea where we will find ourselves.

I hold no brief for transparency saints, but the territorial state is under increasing stress as a viable unit regardless of their antics. This is not, or ought not be, new news. Hedley Bull posed a prospect of the return of medievalism in his 1977 book *The Anarchic Society*, and disquisitions from different perspectives on the growing vulnerability, or impotence, of the territorial state have not since surceased.[2] Some observers have liked the prospect, others not, depending on how they reckon nationalism; still others have tried to hew to the scientific ideal and just describe what they have seen. Yet again, no matter: It is what is it, and the basic reason is clear enough if we just one more time repair to definition—this time of the state.

What does a state have to do to be, and to endure, as a state? It has to do five things.

First, it has to control its territory, which means controlling all agents within it in order to ensure the more or less smooth continuation of ordinary life. This obviously means people, and for that purpose all states have laws and means of enforcing laws; but it also means controlling borders from outsider individuals or armies who would enter unlawfully (national defense), and it means, in theory at least, controlling pathogens that might destroy society (public health), or any other kind of agent that might threaten to do so (extreme scenarios of climate change, perhaps).

Second, a state must obviate civil war, which means it must maintain a monopoly of violence. The origins of the state have to do with a primordial exchange: powerful propertied people (nobles, say) gave up their independent means of coercion (knights in private hire, say) in return for a sovereign agreeing to respect (not expropriate at will) property. That means that competition for wealth and power, which, human nature being what it is, cannot be obviated, must obey rules established by the sovereign, lest factions war upon one another within a defined territory for economic or other reasons. When the sovereign is normatively the people, then a constitution embodies a more or less democratic political system that supplies the same function as long ago did an absolute ruler—a king, a sultan, or what-have-you.

Third, a state must modulate and manage exchanges. Beyond literal defense and security, states establish rules for commerce within and without, and to do that most endeavor to provide some kind of legal and literal infrastructure (courts to adjudicate disputes within, ports and border crossings and customs facilities to facilitate exchanges across frontiers). Without some order to weights and measures, normal life would be too chaotic for any commons. And as all but lighter-than-air libertarians know, all economic activity is based on political frameworks of one kind or another; even "private property" is, after all, a political concept.

Fourth, a state has to finance its own operations. Charles Tilly brilliantly theorized that regime types are partly based on the path-dependency legacies of how different states managed to fund themselves.[3] Yet however they go about it, they must go about it successfully.

Fifth, a state must provide for its own continuity beyond its mortal human agents by having an established means of leadership succession. This means differs, obviously, in different kinds of regimes—monarchy from democracy, and every form in between. But states cannot dissolve or fall to civil war every time a leader passes from the scene and still be a viable state.

Now consider briefly what ransomware piracy events on the scale witnessed earlier this month, and prospectively much larger and more efficacious such events in future, mean in this regard for the five necessary functions of a state:

- Such events diminish state control over what matters in a territory.
- They threaten to give rise to forms of competition the state cannot bring to heel in a court.
- They undermine the management of lawful exchanges.
- To the extent their piracy succeeds, it levies what amounts to a tax on resources that the state cannot prevent and that competes, a little or potentially a lot, with the state's own capacity to raise revenue to sustain itself.
- And in theory they could interfere in political succession processes. After all, if states can hack each other's elections, there is no reason that private actors—political pirates—cannot do the same. This would be not exactly the same as espionage, which Annette Dulzin once described as being to politics

> what infidelity is to marriage; it would be more like an international political orgy, serial and simultaneous infidelity to the protocols of relations among states.

There is something to be said for anarchy. James C. Scott has recently raised *Two Cheers for Anarchism* (2012) and, for that matter, Abdullah Öcalan declared the late Murray Bookchin's anarchist theory of "municipal federalism" the official ideology of the PKK. As a died-in-the-wool anti-statist myself from many years ago—in college I once took umbrage at someone calling Pjotr Krapotkin a "crackpot-tin"—I have some sympathy with this view.[4] I also have some real, matured, practicality-dictated problems with it (hence my view of Assange, Snowden, Manning *et al.*).

But we do have a massive potential governance problem on our hands: The ambit of the territorial state's political control over the actual extent of human transactions, commercial and cultural, aligns less and less with reality in the age of onrushing disintermediation and hyperconnectivity. Something has got to give, and indeed, is already giving. So we need somehow to realign the political with the transactional in a way that preserves democratic accountability as well as, more importantly perhaps, human dignity, autonomy, and a chance to create meaningful work and play.

Now, some people see the so-called populist reaction against globalization, and its handmaiden ideology globalism, as the harbinger of a resuscitation of benign and hopefully liberal nationalism. Given what the ransomware episode of piracy on the cyberseas shows us about the real "state" of affairs, quite a surprise probably awaits such folks. Thanks to what has gone forward with the technology of globalization's newest era, there is now no going back.

But that's fine. The truth is that nationalist sentiment at its 19th and early 20th century heights rarely reposed much emotion in the symbols of the nation or the associated nation-state, except among a tiny bunch of intellectuals. Most people have valued literal community—neighborhood, village, town—much more than nationalist abstractions, and still do. The challenge, then, revealed by the advent of piracy on the cyberseas is to knit together a skein of functional relationships that preserve the social capital inherent in community but that find a way as well to manage the larger governance requirements necessary to protect those communities from harm and even destruction in a dangerous world. Isn't that question worth more than 15 minutes of our attention?

[1] “Governability: A Question of Culture,” *Millennium* (Winter 1992).

[2] One even preceded Bull: Richard J. Barnet and Ronald E. Müller’s *Global Reach: The Power of Multinational Corporations* (1974); and note Saskia Sassen, *Losing Control: Sovereignty in an Age of Globalization* (1996) and her *Territory, Authority, Rights: From Medieval to Global Assemblages* (2006).

[3] See for example Charles Tilly, “Grudging Consent,” *The American Interest* (September/October 2007).

[4] Case in point: See my “A New Pioneer Act,” *National Affairs* (Winter 2016-17).

Adam Garfinkle is editor of *The American Interest*.