# 68 VALDAI PAPERS

June 2017

Valdai Discussion Club
www.valdaiclub.com

A CYBER REVOLT IN THE MAKING

Julien Nocetti
Elena Chernenko

About the authors:

Julien Nocetti

Research Fellow at the French Institute of International Relations (IFRI)

Elena Chernenko

PhD in History, Head of the International Section (Kommersant newspaper), Member of Presidium of the Council on Foreign and Defence Policy (SVOP), Member of the PIR Center Working Group on International Information Security and Global Internet Governance

The views and opinions expressed in this Paper are those of the authors
and do not represent the views of the Valdai Discussion Club, unless explicitly stated otherwise.

A Cyber Revolt in the Making

While all the prerequisites are in place for a global hacker revolt, users seem to be in no hurry to form a "virtual International." What hackers lack is a common goal. All they have is a history of failed attempts to foment a "rise of the machines."

Over the last few months, not a day has passed without the media reporting new, increasingly far-reaching and sophisticated hacking attacks. You could be forgiven for thinking that we are witnessing a global revolt of web users against the powers that be.

However, the opposite is true. For many years, it seemed that the state was relegated to the background in the multi-stakeholder internet governance model, while businesses and civil society were setting the tone. But today, there is no doubt that states are about to take center stage. They have mastered the capabilities offered by cyberspace for domestic and foreign policy, intelligence and military activity. States are now negotiating rules for online behavior, without seeking much input from businesses and ordinary people.

As the state infringes more and more upon user rights and freedoms, whether by censorship or surveillance, it could be argued that a global revolt of hackers is becoming inevitable. The growing "offline" resentment of establishment politics and institutions in the US, EU countries and also post-Soviet states certainly adds credence to this argument.

That said, the cyber mayhem we are currently witnessing falls short of a revolt driven by a political agenda. It is largely the product of rank-and-file cyber criminals and cyber vandals, as well as operations by security forces and dealings within the IT industry.

In this respect, the attribution of the largest DDoS (distributed denial of service) attack in 2016 is quite telling. During the attack, more than 80 popular news websites, social networks and streaming services, including The New York Times, CNN, Amazon, Twitter, Reddit, PayPal, Airbnb, Pinterest, Netflix and Soundcloud, were brought down as a result of sabotage directed at Dyn, a major US domain name provider.

The Dyn attack was carried out in three waves using a botnet made up of more than 100,000 malicious endpoints. Interestingly, these endpoints consisted less of computers than devices from the "internet of things" (IoT), such as gaming consoles, cameras, printers, and even video baby monitors. Four percent of all compromised devices were located in Russia. Some experts claim that the attack strength generated by these devices against Dyn servers reached 1.2Tbps, a level of intensity never seen before in attacks of this kind. The economic fallout from the attack was valued at $110 million.

WikiLeaks, the controversial organization specializing in disclosing classified information, claimed that the Dyn attack was an act of revenge by its supporters for cutting the internet access of the website founder, Julian Assange, who has been hiding in Ecuador's London embassy since 2012. However, cyber security experts questioned whether the hackers, or hacktivists, were politically motivated, especially since WikiLeaks representatives failed to produce any evidence to back their claims.

What researchers do believe is that the attack could be attributable to cyber vandals or Dyn competitors. The fact that code from Mirai malware, which was used to create the botnet, was actively discussed on amateur hacker forums, and the infrastructure used by Mirai had already been used to attack a popular gaming website, supports the first explanation. However, the second explanation could also be right, since ahead of the attack Dyn had come into conflict with a number of IT companies by releasing an analytical report claiming that some anti-virus makers cooperate with hackers who create artificial threats.

Meanwhile, all the technical conditions for a global hackers' revolt are in place, and the political motivation is also there.

Sources of Discontent

Confusedly but inexorably, a generation of activists, or simply citizens, seeks to continue the "democratization" *on* the Internet and *via* the Internet, i.e. by an infinite multiplication of spaces for discussion, an irreversible process that would lead to a questioning of institutions and established positions. Digital technologies offer unlimited possibilities to "act together" – according to the words of German-born American political theorist Hannah Arendt. The word empowerment – barely translatable in other languages – illustrates the boon and the taking up of power by individuals, or groups, in order to act on the political and economic conditions that they endure. The whole society is concerned and all the symbolic fortresses are threatened, including the sacrosanct "exclusive domain" of foreign, defense and security policies.

Increasingly, Western societies are getting through a double process: an unprecedented disaffection of citizens towards a political system, which they no longer identify themselves with, and the incapacity of political institutions to meet this challenge. Facing this multifaceted crisis that "our" system is enduring, the Internet as a tool, media, and personal and collective channel for expression is for some a new opportunity to "recreate trust" among citizens and their rulers, and give back efficiency to institutions.

Digital tools: a response to political disappointment? The deep crisis faced by Western democracies are multifaceted: a crisis of participation – with the rise of abstention and extreme electoral behaviors; a crisis of representation – with the diffuse feeling that a "caste" would have seized power and that politicians no longer understand their fellow citizens; a crisis of the legitimacy of the rulers, together with a crisis of institutions, entangled and hardly understandable. Finally, a crisis of "performance" – with the low respect granted to politics as a means to get progress (as well individual as collective).

A democratic resource? Social media and networks have overwhelmed exchanges between individuals and the relationships between governments and citizens. Twitter, Facebook, VK and their numerous apps give everyone the opportunity to be informed and to inform others in real time. They finalize the split between print and writing, and confirm that virtual proximity has no longer to see with contiguity in space. Visibility, observation, denunciation or repression: Internet has become the "space" for shifting balance of powers, which is also unequal between individual actors or groups, governments, and companies. Its role in electoral processes does not cease to increase. Watchfulness on some hashtags, jointly made by citizens and journalists, can represent a decisive support for mobilizing opposition infuriated by unemployment or corruption.

Indeed, facing the devastating effects of the crisis, diverse mobilizations such as these of the *Indignados* Movement in Spain, launched in May 2011, or the Occupy Wall Street movement, in September 2011 in New York, owe a lot to social networks. Horizontal, reticular, non-institutionalized and non-violent, they distinguish themselves from political parties and trade unions. Inevitably, new protest uses of digital technologies are developing – to which political authorities around the world must adapt to. It is the case with social networks used for coordinating protests, organizing flash mobs, or enabling what famous Spanish sociologist Manuel Castells called "mass self-communication", i.e. the way for an individual to reach a global audience through, for example, posting a video on YouTube or sending a message to a massive email list. The example of the "Umbrella uprising" by Hong-Kong students in winter 2014 shows both a massive and creative use of "all things digital" for political ends. Networked technologies also hinder acts of violence from being kept silent. Police clampdowns in Baltimore, in the USA in 2015 were filmed by mobile phones, and the videos, enhanced with evidence, instantaneously spread on social networks. Such reporters/activists build their own storytelling on the protests, create mobilizing hashtags like #Ferguson or #ICantBreathe that spread worldwide and which some, like #BlackLiveMatters, end on making *Time* magazine's front-page.

Ideology as such is not necessarily absent from the motives of those contesting the *ordre établi*. "Transparency" lies at the heart of the whole "pack" of the libertarian and united values profoundly rooted in the Internet's genes.[1] The biggest private actors of the digital economy also raised transparency as a principle, even as an unsurpassable horizon. Didn't they base their business model on an absolute "mutual transparency" relationship with their users?

Unsurprisingly, the values embedded within the network's hardware and software architectures reflect the context of its creation decades ago, expressing a liberal bias best encapsulated in the notion of a "free flow of information". Perhaps the most important element of the US discourse is the constant linkage between the free flow of information and an open Internet with the goal of preserving and promoting universal human rights to freedom of speech and expression. American policymakers, in both the Bush and Obama administrations, have continuously emphasized the link between the free flow of information with freedom of expression and human rights.[2] Hence the perception, in some countries, that public opinions and citizens around the world are "shaped" by the official US narrative on Internet freedom – although the main effect of Edward Snowden's leaks and the latest Wikileaks revelations completely diluted the US moral authority as a beacon of Internet freedom.

New Threat

The ways and means of involvement deeply diverge according to the actors, between those who stick to legality and those who consider necessary to infringe the law.

For instance, it is hard to compare the actions of WikiLeaks, Anonymous, or Telecomix. It is thus necessary to comprehend the political motivations that drive these various groups or initiatives.

WikiLeaks is now directly tied to the personalities of Julian Assange, entrenched in the Embassy of Ecuador in London since almost 7 years, and Chelsea (formerly Bradley) Manning, sentenced in August 2013 to 35 years in prison for having leaked classified documents. WikiLeaks unashamedly contests the principle of *raison d'Etat*, and presents

[1] *Fred TURNER, From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network and the Rise of Digital Utopianism, Chicago: University of Chicago Press, 2006.*

[2] *Daniel McCARTHY, Power, information technology, and international relations theory. The power and politics of US foreign policy and the internet, Basingstoke: Palgrave Mcmillan, 2015.*

itself as a counter power. Back in 2010 the affair brutally illustrated a series of "breaks": between the privilege of confidentiality of the elites and the need for transparency of the masses; between the monopoly of political decision-making and the desire for a better-shared democracy; and between a ruling caste seated on concealment and younger generations for whom Facebook represents a new grid of understanding the world.

It is worth noting in this respect that WikiLeaks failed in its efforts to shake up global politics by publishing classified documents about the US military operations in Iraq and Afghanistan, as well as diplomatic cables. When WikiLeaks was only beginning to release the papers in its possession, many thought it would lead to tectonic shifts. Italy's foreign minister at the time, Franco Frattini, had the most memorable quote along these lines: "It will be the September 11th of world diplomacy." Julian Assange himself claimed that the revelations would blow up the system. However, not a single country cut off diplomatic relations with another, and not a single government resigned. There have been a number of other major leaks since then (and they continue), however they have had less impact on global politics than has been expected. For instance, the revelation that US intelligence agencies wiretapped German Federal Chancellor Angela Merkel's cellphone for quite a while did not stop her from visiting the US. High-ranking representatives of G20 countries did not refuse to take part in G20 summits, although it is not uncommon for host countries to use events like this to access computers and gadgets of delegation members (as was the case in Great Britain in 2009). Countries have become more or less resistant to such leaks.

However, these revelations did have an undeniable effect: they undermined popular trust in political leaders and institutions. The discontent and commitment to protect their right to know led the most advanced computer users to become hacktivists, since they had no other way to influence global politics and intelligence agencies.

The Anonymous group, probably the most famous hacktivist movement, refers to highly diversified communities of Internet users that present themselves as defenders of the right to free expression online and beyond. It is a "galaxy" that nowadays seems more preoccupied to play with computer flaws of organizations rather than to carry a political project. Still, Anonymous has so far provided the only actual example of a global cyber revolt. WikiLeaks and Anonymous brought their support to Edward Snowden, who obtained a temporary asylum in Russia since July 2013; he arrived there with Sarah Harrison, WikiLeaks' legal advisor. Snowden's revelations have been made through major international newspapers. Less covered by the media, Telecomix has led actions seeking to bring back communications means following "switch off" decisions made by some regimes which resorted to repression to quell the contest as in Tunisia, Egypt or Syria.

The "Internet culture", that started to take shape in the second half of the 1960s, is simultaneously irrigated by two sources, closer than it might first seem in view of the organization of US research: a military-scientific source at the root of Arpanet, and an anti-establishment source denouncing in particular the US military involvement in Vietnam. The "Internet culture" resembles a counter-culture which lies on the principle of sharing and linkage; extremely diverse, it is conveyed by authentic liberals (in the American sense of the word), libertarians, radical anti-capitalists, anarchists, pure geeks or, more simply, Internet users defending their freedom of expression, linkage and organization[3]. In this regard, one may establish a historical parallel between the Snowden affair and the *Pentagon Papers*, starting point of Hannah Arendt's thought to understand "the processes where governmental decisions are entangled" and the mechanisms through which decision-makers produce "deception"[4]. In 1971, Daniel Ellsberg, a RAND Corporation analyst, handed 7.000 pages of classified documents to *The New York Times* describing the successive conditions of US involvement in Vietnam. Logically, he supported Julian Assange and Chelsea Manning. In a 2013 op-ed Daniel Ellsberg claimed that the American intelligence services have a strike force and privacy violation "which is today incomparably more powerful than everything prior to the pre-digital age". According to him, Edward Snowden "risked [his] life" to disclose information touching to the most fundamental individual and public freedoms; he should incite "others having the same knowledge, the same consciousness, and the same patriotism, to demonstrate a similar civic courage".[5] Late September 2013, a draft reform of the NSA was launched by the US Parliament, in order to put "limits" to the surveillance programs while "preserving" their efficiency.

Inevitably, for intelligence services –in authoritarian regimes as well as in democratic systems – the risk is real to see unfolding of a "digital wave" as the main threat: since September 11, the fight against international terrorism – i.e. against Al-Qaida – has been presented to world opinions as the main threat. The Snowden affair has seemingly triggered a change of paradigm, without this latter be subject to any public debate[6].

First Wave

So far, only one such wave, the Anonymous movement in 2010–2011, can be viewed as a real hacking revolt. Back then, thousands of hackers and ordinary users from across

[3] *Joshua FOUST, "The Geek Awakening, Edward Snowden is the vanguard of a broader challenge", Medium.com, 4 July 2013.*

[4] *Hannah ARENDT, Crises of the Republic, New York: Mariner Books, 1972.*

[5] *Daniel ELLSBERG, "Aux Etats-Unis, une cybersurveillance digne d'un Etat policier", Le Monde, 26 July 2013.*

[6] *Thomas GOMART, "Aux démocraties de montrer l'exemple", Le Monde, 30 October 2013.*

the world came together to punish the US and a number of other countries for pressuring WikiLeaks. Many regarded WikiLeaks founder Julian Assange as the main fighter for the freedom of speech, while the website he created was expected to signal the dawning of a new era in which governments would no longer be able to conceal information from their citizens. Outraged by the online disclosure of hundreds of thousands of secret documents, the US tried to force companies to stop working with WikiLeaks. A number of major payment and hosting providers bowed to pressure from Washington, making it much harder for Julian Assange to receive donations and keep the site running.

This was when Anonymous stepped in to support WikiLeaks. By 2010–2011, the movement had already existed for several years, but was known only within a restricted circle, mainly for successfully breaking into Scientologists' online resources or supporting the Pirate Bay torrent tracker. Anonymous members gathered thousands of users under their banners in Operation Payback. As their slogan, they chose a quote by John Perry Barlow, one of the founders of the Electronic Frontier Foundation: "The first serious infowar is now engaged. The field of battle is WikiLeaks. You are the troops".[7]

Anyone was welcome to contribute to attacks on websites hostile to WikiLeaks, since step-by-step instructions on carrying out DDoS attacks using Low Orbit Ion Cannon (LOIC), a simple piece of software, were freely available on hacking websites and on Twitter. This resulted in users from all continents joining attacks against the websites of Mastercard, Visa, Paypal and Amazon, a majority of whom had never been involved in hacking before.

The campaign's success was guaranteed by its sheer scale. A number of government and corporate resources were temporarily put out of operation. In 2012, Time magazine listed Anonymous among the top 100 most influential people in the world.

Back then, many experts believed that hacktivism would gain traction moving forward, and that this would be the way users driven by a political agenda would respond to any injustice[8]. However, the wave soon receded, and never reemerged on a similar scale.

There are several reasons why the first cyber revolt was not followed by others. First, Anonymous lacked a leader or a core that could coordinate joint action and motivate members to remain engaged. Any Anonymous member could speak out for the movement in the media. Online discussions to agree on the goals and timeframe of attacks were also quite chaotic, and the first successful attacks gave rise to heated debates on future targets.

[7] *John PERRY BARLOW, tweet posted from @JPBarlow on 3 December 2010.*

[8] *See for instance Galina MIKHAYLOVA, "The Anonymous movement: hacktivism as an emerging form of political participation" https://digital.library.txstate.edu/bitstream/handle/10877/5378/MIKHAYLOVA-THESIS-2014.pdf?sequence=1; and Victoria MCLAUGHLIN, "Anonymous: What do we have to fear from hacktivism, the lulz, and the hive mind? ", https://pages.shanti.virginia.edu/Victoria_McLaughlin/files/2012/04/McLaughlin_PST_Thesis_2012.pdf*

While most Anonymous hackers in the West continued to attack websites of payment systems that refused to work with WikiLeaks, calls emerged among Russian hacktivists to strike the Pentagon.

Second, many early Julian Assange sympathizers soon became disillusioned. Some were scared off by the rape charges brought against the WikiLeaks founder, while others were perplexed by the departure from WikiLeaks of key staff, who accused Assange of misappropriating millions in donations. There were also those who did not agree with Julian Assange's decision to release classified documents without censoring names and addresses, despite the fact that it put some of the people mentioned in the documents in harm's way (for example, US informants in Afghanistan).

Third, as soon as Anonymous started actively recruiting people on Facebook and Twitter, their accounts were disabled, while websites like Anonops.net were put out of operation for a long time. Deprived of communication tools, Anonymous struggled to reconstitute itself. The very environment that made the emergence of hacktivists possible turned out to be their Achilles' heel.

Finally, the fact that US law enforcement agencies went after the movement's members had a clear chilling effect. After several high-profile arrests and show trials, the number of those willing to take part in attacks sharply dropped. It is telling that even the hacktivists' idol, John Perry Barlow, condemned them, calling DDoS attacks "the poison gas of cyberspace."

Anonymous prepared and carried out a number of other operations, which were no longer related to WikiLeaks and all much smaller in scale compared to Operation Payback. Today, several separate groups operate under the Anonymous brand, and most of them are hacking just for the "lulz".

The fact that the first wave of hacktivism died out does not mean that a second or third wave will not follow. The future of this movement will to a large extent depend on the existence of a unifying cause like WikiLeaks, which prompted the Anonymous community to stand up for its rights. It can be even argued that next time it would be even easier to bring people together, since they would have a clear vision of what they can achieve together. Next time, they may even go beyond DDoS attacks.

When the movement was still alive, its most active members were discussing whether to engage in a different kind of action. For example, experienced hackers could stage defacement attacks to change the visual appearance of the targeted websites and post there calls for protests or similar information. Amateur hacktivists could then help raise awareness about these attacks on social media, messenger services, etc. Another option was for advanced hackers to break into email accounts of officials or government agencies, download correspondence, while rank-and-file activists would read it to find compromising information and help spread the word. Anonymous has even carried out several operations of this kind, including when they broke into the email server of Stratfor, a private US geopolitical intelligence platform, and leaked 200 gigabytes of correspondence to WikiLeaks. WikiLeaks got hold of correspondence of Bashar al-Assad's associated the same way.

Nonetheless, regarding the attack against the email server of the Democratic National Committee and accounts of people close to former US presidential candidate Hilary Clinton, Julian Assange said that neither hacktivists, nor Russian intelligence services (as the US authorities claim) were behind the leak, which reportedly came from an insider.

#Valdaiclub

ValdaiClub

ValdaiClub

valdaiclub.com

valdai@valdaiclub.com

ISBN 978-5-906757-53-1

9 785906 757531

Council on Foreign and Defense Policy

RIAC Russian International Affairs Council

MGIMO UNIVERSITY

HIGHER SCHOOL OF ECONOMICS NATIONAL RESEARCH UNIVERSITY