A (Guided) Tour of the Digital Wild West

Xavier Raufer

Abstract

Criminology now operates across two different worlds: the *physical* and the *digital*. Separate, yet linked in mutual observation and imitation, these two worlds frequently intertwine. While still a source of concern, physical crime, including terrorism, is under at least a degree of control. In contrast, in the digital universe, criminal chaos runs wild, and society has not even begun to recognize the real dangers this will soon bring.

Keywords: cybercrime, Cyber Far West, cyberattacks, GAFA

Tour (guiado) del salvaje oeste digital

Resumen

La criminología ahora opera en dos mundos diferentes: el físico y el digital. Separados, pero vinculados en la observación mutua y la imitación, estos dos mundos se entrelazan con frecuencia. Aunque sigue siendo motivo de preocupación, los delitos físicos, incluido el terrorismo, están bajo al menos un cierto grado de control. En contraste, en el universo digital, el caos criminal se vuelve salvaje, y la sociedad ni siquiera ha comenzado a reconocer los peligros reales que esto traerá pronto.

Palabras clave: cibercrimen, Ciber Far West, ciberataques, GAFA

数字蛮荒地带指南

摘要

当前犯罪学的运行跨越两个不同世界：现实世界和数字世界。相互分离却又通过互相观察和模仿产生联系，这两个世界频繁地交织在一起。尽管依旧是一个顾虑源，但包括恐怖主义在内的现实犯罪至少在一定程度上受到控制。相反，在数字世界中，犯罪事件迅速蔓延，并且社会甚至还来不及意识到其很快将带来的真实危险。

关键词：网络犯罪，Cyber Far West，网络攻击，GAFA

 doi: 10.18278/ijc.7.1.5

Introduction

Criminology now operates across two different worlds: the *physical* and the *digital*. Separate, yet linked in mutual observation and imitation, these two worlds frequently intertwine. While still a source of concern, physical crime, including terrorism, is under at least a degree of control. In contrast, in the digital universe, criminal chaos runs wild, and society has not even begun to recognize the real dangers this will soon bring. To outline:

- The worst cyberattacks are almost never met with any response, so they grow in number and in severity.

- To date, the major world powers have not conceived of an effective means of countering the most serious attacks. These powers are incapable of even defining digital attacks and when they might constitute an act of war, being unable to even reach an agreement as to what is or is not permissible in cyberspace! Except in the (ever-present) case of child pornography, in cyberspace no obligatory norms or rules exist. President Emmanuel Macron has stated that "we need to be tough and have clear rules," but society is weak on this, and at present chaos reigns.

In short, every attempt to regulate cyberspace has failed to stop it becoming, in the words of former US President Barack Obama, a chaotic and anarchic "wild, wild West," where anybody can loot and pillage at will, with minimal risk to themselves.

In France, meanwhile, this worrying truth tends to disappear behind a façade of self-satisfaction. In its reports, the country's official apparatus tasked with fighting against cyberthreats seems perfectly happy with itself. Each document seems to have been cast from the same mold:

- First, a brief, general, fine-sounding introduction about the disordered nature of cyberspace, carefully avoiding awkward details and anything too troubling;

- Then, a proclamation of Grand Principles and Noble Values warning humankind and cyberspace that from now on they will have to respect the norms, rules, needs, habits, and customs of the French authorities;

- Finally, the essential point: the construction of a geometrically harmonious textual Parthenon, thirty percent devoted to confronting the problem, and seventy percent to extending the remit and powers of the agency in question.

What do we find in the one hundred and sixty-seven pages of the recent *Revue Stratégique de cyberdéfense* [Strategic Review of Cyberdefense], published in February 2018? What does it have to say about the enemy, the hackers, the hostile state that infiltrates, sabotages or spies on our networks? What of the for-

eign agents, the mafias? Nothing. Sabotage, theft, espionage, and destabilization? Check. Risks and vulnerabilities? Check (naturally). But what of the attackers themselves? In the distance, just around the next turn of phrase, some irritating troublemaker occasionally slips into view and then disappears, giving the impression that the threat the country faces is a phantom one.

At the end of the *Revue*, there are seventy-seven references, notes, sources, and so on. There is nothing about the actors in cybercrime, hackers or otherwise. The *Revue* is a prisoner of what is known in phenomenology as "the sphere of the calculable," or "if it can't be counted, it doesn't count." Hence my questions: If we do not know our enemy, how can we "build the peace and security of international cyberspace"? How can we "anticipate," "prevent," or "detect," attacks if we do not know WHO to watch, who to put under surveillance—if we overlook the NATURE of the cyberthreat?

Moving to specifics: "Protecting our information systems"—against whom? "An active stance of attack deterrence and coordinated response" and "digital sovereignty"—in relation to whom? "Effective penal response"—to imprison whom? "Prevention ... Anticipation ... Detection ... Attribution ... Reaction"—how can this be achieved without a known and identified adversary?

There do exist services that look after the people of France's fundamental interests. First, the Direction générale de la sécurité intérieure (DGSI) (Directorate General for Internal Security), which, we learn, is "beefing up its cyber investigation capabilities" (*Le Monde*, June 5 2018), as part of a project to create a "national *technical* service for criminal information capture" (Service technique national de captation judiciaire, STNCJ). But is confronting cyber predators merely a *technical* matter? Are the "cyberattacks [that are] growing in number, intensity and sophistication" (*Strategic Review of Cyberdefense,* February 2018) not due to actual cyberattackers, who need to be named and exposed? Are the criminally weaponized computers not under the control of gangs and networks of flesh-and-blood hackers, criminals, and hybrid actors, all of whom must be found and infiltrated? Is our attitude to cyberdefense not somewhat Platonic?

But this irenic reaction to cyber banditry is not unique to France. It can be found across the European Union (EU), among whose goals is to set up a digital single market across its member states. For European Cyber Security Month, October 2015, the EU's relevant body, the European Union Agency for Network and Information Security (ENISA), published a list of forty educational programs and diplomas, three hundred seventy-five different courses in all, available in most EU countries.[1] The content of these courses? Once again, only measurable and countable aspects: network, system, hardware, and software security, IT and forensic

1 Including Germany, Austria, Bulgaria, Cyprus, Spain, Finland, France, the United Kingdom, Greece, Hungary, Ireland, Italy, Luxembourg, Norway, the Netherlands, Poland, Portugal, Romania, and Sweden.

sciences, cryptography, the audit and security of the technical aspects of information and communication processes, information management and security, IT security protocols, and so on. Who is the (digital) enemy? Where are they? What are they doing today, and what will they be doing tomorrow? There is nothing on this, nothing of substance on the hackers, the spies, or the saboteurs. We are fighting thin air.

This study does not overlook this enemy. Adopting a battle cry of "back to the things themselves!" (à la Edmund Husserl), let us head into enemy territory.

Prologue: Silicon Valley Man, How Fragile Thou Art[2]

"No countries, no borders": an unexpected reprise of the Comintern dream. In the post-hippy Californian kaleidoscope of Silicon Valley, the good life comes with no ties. It is mobile, flexible, and fluid. It is Ayn Rand-style egotistical anarchism for rich kids, the libertarian myth of the transitory, of mobility, of the absolute ME. It is a puerile dream: never get bored, escape from routine, do whatever you want, go and live in a tribe, as a neo-hunter-gatherer; six months in a shared office in Berlin ... spend the summer (which one?) in a caravan in Chile ... the rest of the time at a start-up incubator in New York. Today, designing software for a bank in Myanmar, tomorrow launching a new brand in Saudi Arabia. Are these international globe-trotting entrepreneurs inhabiting a new kingdom of the chosen? In reality, they are ideal targets for criminal networks, hackers, and providers of special services, intent on looting their lovely digital world, championed by blind "snowflakes," all eternally adolescent Peter Pan clones.

The Evils and the Wonders of Silicon Valley

An opening statement: anyone who has managed to escape from what is known in phenomenology as "the sphere of common knowledge" will be anything but surprised at the domination of the "tech titans" depicted below. Decidedly the opposite, in fact, particularly if they have read the following prophetic statement from 1966, just over half a century ago:

> At present, we reflect on the phenomenon of steering. This phenomenon has today, in the age of cybernetics, become so fundamental that it occupies and determines the whole of natural science and the behavior of humans [...] That natural science and our life today become ruled by cybernetics in increasing measure is not accidental; rather, it is foreshadowed in the historical origin of modern knowledge and technology. (Heidegger and Fink 1979, 12)

2 I urge you to read Alastair Bonnett's splendid *Beyond the Map: Unruly Enclaves, Ghostly Places, Emerging Lands, and Our Search for New Utopias* (Chicago: University of Chicago Press, 2018).

In the world we live in, somewhat removed from the philosophical realm, the institutions, military command structures, and so on that are put in place to combat digital violations tend very much to follow a narrowly technical approach, and France is no exception. Unable to conceive of anything but objective constraints and needs, engineers normally only address the kinds of problems to which an engineer might have a solution. At the heart of this approach is the Newtonian theory of the perfect mechanism: malfunctions and breakdowns can occur, but technical perfection can be restored by performing suitable repair work. An engineer looks at cyberspace and sees a virtuous and reliable clockwork mechanism. If a gremlin appears in the works, repairs are carried out and order is restored.

But a roulette wheel is, of course, *inherently designed* to work against the interests of the player; the best engineers in the world cannot make "virtuous" a machine whose main function is to cheat. While extremely competent in what they do, our cyber engineers struggle to understand this. In their profound honesty, they pass over the fact that cyberspace does not spring from some pure and unspoiled Creation, with the aim (as claimed in the skewed promotional material) of "making the world a better place," of "making things more open and connected," in the hope of delivering it from its present suffering and afflictions. Much more realistically, cyberspace is fundamentally the fief of cynical libertarian titans, whose only aim is to amass billions while remaining utterly indifferent to criminal activity, hacking, and the shameless plundering of their customers' private data.

Is this an exaggeration? Not at all. To begin with, let us look at some shocking examples of the true nature of GAFA (Google, Apple, Facebook, and Amazon). All of these examples involve Facebook, although the others are no better:

- In the early days of Facebook, a journalist asked its CEO, Mark Zuckerberg, why the public would trust him with all their personal data. Confirmed libertarian Zuckerberg gave a very clear response: "They trust me. Dumb fucks."

- On April 28, 2018, a photo of Facebook's headquarters appeared in the *New York Times International Edition*. Clearly visible was the address—freely chosen by the company itself, naturally: 1, Hacker Way. Just in case things were not yet clear enough ...

- In early 2018, a researcher discovered some one hundred twenty forums and discussion groups on Facebook (with around 300,000—yes, *three hundred thousand*–participants in all) dedicated to cybercrime and hacking, all offering each other software and intrusion tools or digital robbery, in plain view of the whole world. Why hide on the Dark Web when Facebook is so very welcoming?

The imposing titans of the internet have ideologies and practices akin to those of hackers. These are the foundations of all cybercriminology. This study

begins, then, by inviting the reader to open his or her eyes and take a good look at these tech titans.

The Titans of Technocapitalism: More Powerful than Nation States

What follows is not about innovative companies enjoying well-deserved success. It is about online monopolies embarked on a ruthless "uberization" of the world.

The US stock market has been growing continuously for the last nine years, thanks solely to GAFA. Between January and June 2018, 50 percent of company profits listed on Standard & Poor's 500 Index came from Facebook, Alphabet (Google), Apple, Amazon, and Netflix.

Apple was founded in 1976, and in August 2018 its market capitalization passed the trillion-dollar mark. But twenty years ago, Apple was no more than a medium-sized business designing high-end computers.

Facebook had 100 million users in 2008. By 2018, it had 2.1 billion. The company captures 77 percent of the world's mobile social network traffic.

In 2007, Amazon employed 17,000 people. By 2017, it employed 542,000. HALF of all the e-commerce in the world takes place via their mega-servers.

Apple and Google provide the software (programs, applications, and so on) for 99 percent of the world's smartphones. Google has an 81 percent share of the global search engine market.

Facebook and Google between them hoover up 59 cents in every online advertising dollar. They also carry 63 percent of all digital advertising in the United States. In 2017, 89 percent of the growth in turnover of the online advertising sector went to these same two companies.

GAFA Ideology: The Fox in the Henhouse

A recent study (*New York Times International,* October 18 2017) revealed the political views of six-hundred influential American high-tech directors and senior executives, one third of whom were based in and around Silicon Valley. As one might have expected, they are overwhelmingly libertarian and are in favor of total deregulation and unlimited migration (cheap slaves are always in demand. . .). Equally obviously, they are fiercely hostile toward all state supervision and are in favor of the unlimited ability to fire personnel: entrepreneurs must be perfectly free to operate in their market. Thus unencumbered by any societal costs, these exalted individuals are free to be ardent supporters of every fashionable idea: free access to drugs and abortion, the glorification of LGBT causes, and so on.

But when it comes to business, these directors and senior executives are clearly not such nice-guy progressives. Just consider the profiles of the 2 billion users of Facebook, which contain around one hundred items of information: race

(supposedly non-existent), sex (supposedly replaced by "gender fluidity"), income, financial standing, value of primary residence, whether they have family, whether they have teenage children or not, loans taken out, whether they observe Ramadan (!), their vehicles and when they were bought, and so on. Each and every profile has been sold to advertisers, bringing Facebook, through those intrusive "Ad Preferences," somewhere between one and three billion dollars every quarter.

Behind the shiny, happy post-hippy-all-brothers-and-equals image, the private data extorted—in the darkest of shadows, because "transparency" is for losers—from 2 billion customers, subscribers, and others are subjected to immensely detailed manipulation, which provides the constituent members of GAFA with the most formidable concentration of coercive power in history. As of today, GAFA is colonizing networked humanity, reaching into your lounge, your bedroom, your dining room, kitchen, and office—right down into your pocket.

The Incestuous Relationship Between GAFA "Libertarians" and the Pentagon, CIA, and Others

Amazon created the cloud used by the American intelligence community; Microsoft devised the "Azure Government Secret" cloud (for the use of federal government, individual states, the Pentagon, and so on); Google is piloting the Pentagon's artificial intelligence project, and so on. Which joker coined the term "net neutrality"?

An Iron Grip on Global Information and Media

> Never neutral, technology is always molded by the values of those who create it. In the case of Blockchain-based cryptocurrencies, those values are libertarian and mechanistic; trust in them depends on algorithms; state and other forms of regulation are viewed with suspicion and hostility. (*New York Review of Books*, January 18 2018)

A few anonymous individuals now decide how the planet gets its information, how it consumes, and how it communicates. Facebook is truly the "editor-in-chief of the Earth": 45 percent of Americans access news via this platform, while another 25 percent do so via Google. In this way, between them, these two private companies control the news environment of billions of the Earth's inhabitants. One more demonstration of how right Marx and Engels were: "The ideas of the ruling class are in every epoch the ruling ideas, i.e. the class which is the ruling *material* force of society, is at the same time its ruling *intellectual* force" (Marx and Engels, 1968 [1846]).

GAFA: Utter Disregard for Crime and Individuals' Security

A 2017 *New York Times* article (*New York Times International,* October 20 2017) told how 324 hectares of a large district of Toronto is to be restructured. "Sidewalk labs" (Google's urban redevelopment studio) has got in on the act. Underpinning its project is the boho-libertarian mantra: "friction = bad; diversity = good; fluidity = better still." The area will be carbon-neutral, with cleaning, recycling, noise, and pollution all monitored and run by high-tech control systems. Taxis and deliveries? Robots. Around the modular buildings, sidewalks and streets will be warmed by cutting-edge heating systems that melt the snow.

The shiny new future is now within reach. Except that at the same time, Toronto is experiencing a huge rise in crime. As this is a Google project, why not use Google to search "Toronto crime"? Dozens of articles appear for our edification. But like the rest of Silicon Valley, Google does not care about crime and the security of the citizen. Fixated on the calculable, and having failed to consult its own search engine, Google does not know—or does not deign to recognize—that around its "modular buildings" and along its "heated sidewalks" lie bodies riddled with bullets. One among no doubt many niggling examples of "friction."

Classic Vices Behind the Mirage of a "New World"

Beneath the gospel of humanity's marvelous digital future, there lies a less glowing reality: the tech titans of the day behave just like the good old capitalists of yesteryear: employees and sub-contractors alienated through social engineering; sexual favors extracted in return for jobs or money; and a blind eye turned to crooks and conmen like themselves.

- *Silicon Valley is a slave driver* (*New York Times*, September 6 2017). There is a fascination with "toys for adults" ... paeans to wealth bordering on brainwashing ... the worship of work-addiction ... "burnout suicides" and euphoric episodes ... "Wanna buy your own plane?" Easy: work 18 hours a day, no holidays, no parties, no meals out, no friends, no family, no children, no time to be young, no sleep. A T-shirt popular in Silicon Valley reads: "9 to 5 is for the weak." All in order to stand out at the courts of the tech titans. Do or die—what does it matter? Thousands of young dupes flood into the Valley every year. The propaganda makes sure of that.

- *Puritanism and "diversity" are for the masses*. Outwardly, the Silicon Valley elite adhere to all the inclusive "values" of the day: LGBT (and other) rights, "diversity," antiracism, feminism, veganism, and so on. In the Valley, anyone who challenges this smothering ideology is banished from the digital Eden. Outwardly, that is, because once again, behind the mirage of a new world, the worst excesses of the old persist. Nothing has changed since the rise of "sport f*cking" in the 1970s (*CBS News*, February 10, 2018; *Vanity Fair*, January 2

2018). Beneath the prudish exterior of Silicon Valley, recent investigations have uncovered the orgy culture that is rife in the boys' clubs shared by the male CEOs, commercial bankers, and directors of high-tech, real estate, and advertising firms. At the weekend, these titans, with their paleo-hippy mindset, "invite" their female employees—or those from nearby start-ups—to *soirées* of sex, drugs, and power in secluded villas or hotel suites. But if you work in the Valley, how can you turn down an "invitation" from those who control your future? And who attends these secret orgies? Younger women and older men (always white and heterosexual) in a ratio of two-to-one. "Diversity"? That's for the press releases only.

- *Cyber fraud is still fraud*. Might we see a high-tech Bernie Madoff? With all the data, the "transparency," and the monitoring of online activity? Impossible? No. The young self-made woman Elizabeth Holmes had founded and was running the start-up Theranos, working to revolutionize blood testing: a laboratory on the tip of a needle, thanks to her technological solution, "Edison," which would carry out hundreds of tests in an instant, with just one drop of blood. This would have saved American health insurance programs such as Medicare and Medicaid hundreds of millions of dollars. Theranos promised the moon, and the media fell for it hook, line, and sinker. The story appeared on the front cover of *Fortune Magazine*, *Forbes*, and *Time*. So came the cries: Holmes is one of the richest and most influential women in the world! She's a media darling! Henry Kissinger's on the Board! Nine-hundred million dollars of risk-capital poured into the miracle start-up. Such credulity, such gullibility, such blindness, and it all turned out to be a sham. Silicon Valley, the media, the investors, and the customers were all scammed, old-school.

Cyberconflict, Present and Future

At present, the term "cyberconflict" suggests a digital Cold War: undeclared; surreptitious, indirect disruption; an arms race, just in case. But the cast is now different from what we saw during the two-sided Cold War. Today we have North Korea's cyberarmy of around six thousand hackers, capable of stealing (or recovering) the NSA's digital offensive weapons and modifying them in order to loot poorly protected banks (to make ends meet); or sabotaging the computers of anyone who dares to disrespect the "Great Leader." In a world where everyone is always talking about detection and prevention, it has to be pointed out in passing that not one misdeed on the part of Pyongyang has ever been identified or foreseen by anybody, with the planet's global gaggle of cyber experts floundering around for months before dimly spotting the problem.

These episodes do demonstrate, however, that cyberconflict is an ideal arena for asymmetric strategy: it is cheap, anonymous, even profitable, and poses a

threat to the infrastructure of the developed countries. This point, rarely addressed in our equivocal approach to cyberdefense, is a very important one. It may best be illustrated by imagining the scene shortly after a successful blitz attack on the critical energy infrastructure of a typical modern country. With all such infrastructure now one hundred percent computerized, the country is effectively unplugged and in meltdown before the first shot is fired, resulting in:

- deletion of crucial data
- theft of sensitive information
- paralysis of critical infrastructure
- diminished military capability
- no electrical power for offices and homes
- no telecom services, cell-phone networks, or internet access
- no emergency services or law enforcement
- no trains or subways
- non-functioning equipment in hospitals and medical centers
- no traffic lights
- no financial networks, card payments, or ATMs
- no gas at gas stations
- bank accounts are inaccessible
- no control of hydraulic dams, wind farms, or solar farms
- closure of wastewater treatment plants (domestic and industrial)
- no way of calling the police (leading to riots and mass looting)
- no refrigerators and no supply chain to supermarkets (with food supplies used up within a week)

According to one expert, "[t]o hackers like these, we are like Bambi in the woods." At the very least, the United States, Russia, and China have the ability to mount such attacks, any response to which is rendered impossible: in cyberspace, there is no such thing as deterrence.

When hackers are detected in a critical network, they no longer run away like they did in the past, politely closing the door behind them. Now, they dig in

and shoot back. Experts describe this in the language of trench warfare, like something akin to a close-quarter knife-fight (Report by the Office of the US Director of National Intelligence, May 2018). The following are three current examples of strategic cyberattacks:

- Federal Government of the United States, Office of Personnel Management: every federal employee has a digital dossier (Standard Form 86), which contains details about their entire life: a list of every foreigner they have come into contact with since childhood, parents, partner(s), children, family, anyone with whom the person concerned has any association at all, licit or otherwise, and their medical and financial profile. In June 2015, the OPM announced that twenty-one million (that's right, million) of these SF86 dossiers had been hacked. By whom? Umm, ... the Chinese, maybe?

- August 2017, Saudi Arabia: a cyberattack on a petrochemical plant belonging to a large international company closed down operations using a minor "bug." Targeting the controls of the plant's key functions, this sophisticated digital attack required specialist knowledge of its design and layout. The idea was not to sabotage the plant, but to make it explode, as happened in the 1984 Bhopal disaster. The design of the plant (by Schneider Electric) is similar to that of some eighteen thousand others around the world (nuclear, petrochemical, water treatment, gas, industrial chemicals, and so on).

- A software system known as ECDIS (Electronic Chart Display), commonly used in commercial shipping, (cargo vessels, tankers, and so on) can, via remote hacking, be made to distort a boat's size and position on neighboring vessels' GPS tracking systems by up to 300 meters. ECDIS then triggers the alarm-collision feature of the Automatic Identification System. Interference of this kind, applied to several ships in close proximity, can quickly paralyze any confined area of water, such as the English Channel.

Hackers and Hacking: Present and Future

> Our virtual world, whether it is a company information system, an industrial network, or very simply your family computer, has never been so vulnerable, attacked on all sides without any sign of the problem being solved. (Interview with a cybersecurity expert, SDBR, April 3 2018)

The Cause of the Disaster: The NSA

From 2016 onward, Tailored Access Operations (TAO), the NSA's most secret division, responsible for all offensive/intrusive aspects of target information systems,

has been hacked repeatedly. Considered by the Congressional Commission of Inquiry to have been a total debacle—the worst shock in the history of American Intelligence—TAO was penetrated to its very heart, eviscerated. According to the Commission of Inquiry, the hackers, known as the Shadow Brokers, now know everything, or nearly everything, about the NSA's secret operations. In contrast, even after eighteen months of internal investigation, Washington knows nothing about them—not even the magnitude of the theft. Are they brilliant hackers? Moles? Both? Nobody knows. Among other things, the Shadow Brokers have stolen all the NSA's cyber weapons designed for breaking through Windows and Linux firewalls.

The CIA is in no position to smirk, either. Its cyber intelligence has also been penetrated, and its secret documents subsequently passed, en masse, to Wikileaks—by whom? Once again, no idea. Then the NSA's cyber weapons EternalBlue and DoublePulsar found their way, perhaps sold, perhaps quietly smuggled out, to some Chinese, Russian, or North Korean hackers, who are probably not particularly hostile toward their own official agencies. And finally, these hackers put together virulent ransomware (including WannaCry and NotPetya) that has been ravaging the digital world since May 2017, blocking millions of computers, and so on.

According to American insurance giant AIG, a big player in commercial cyber risk, 2017 saw an explosive rise of more than 26 percent in ransomware attacks (WannaCry etc.), probably carried out with state involvement. The company estimates that the damage inflicted worldwide runs to 8 billion dollars.

In spring 2017, Action Fraud (the UK's national fraud and cybercrime reporting center) reported a sudden spike in online cyber fraud (alongside WannaCry attacks), rendering the digital security profession completely exposed: more than 63 percent of reported episodes came from the business sector.

The Fundamentals of Hacking Going Forward

For experts, the term "cybercrime" covers a range of offenses, the foremost being:

- identity theft (real identities of real, physical persons)
- creation and use of fake identities (representing fictitious persons, and able to pass the security checks of target organizations)

(These two kinds of identity fraud enable a whole range of thefts and scams, losing US banks around 2 billion dollars a year.)

- use of ransomware to "kidnap"—that is, "encrypt"—data on servers belonging to a company, a government department, or a municipal authority, and so on, and releasing them in return for a payment in cryptocurrency.
- a range of digital incursions against companies and others in order to carry

out espionage or blackmail, find compromising information, or gain an unfair market advantage, and so on.

Some British academic researchers contend that criminal e-commerce now has its own mega-servers—a kind of illicit Amazon or Facebook—which transact over 1,500 billion dollars of business a year, similar to the gross national product (GNP) of Russia. Indeed, they claim that if "black market cyber capitalism" were a country, it would be the thirteenth biggest in the world by GNP.

Through these mega-servers, which typically operate on the dark net, a huge and ever-increasing clientele can gain easy access to drugs, weapons, ammunition, explosives, hacking tools, illegal services, expert opinion from hackers, and training in online fraud.

As with any well-managed system, these criminal mega-servers spend around 300 billion dollars per year on improving their sites and their technical infrastructure, on streamlining their customer interactions, optimizing their "customer experience," and so on. Of the 1,500 billion plus dollars a year that these mega-servers transact:

- black market trading (illegal online markets) : 860 billion USD
- hacking, theft of intellectual property : 500 billion USD
- espionage, sale of stolen data : 160 billion USD
- sale of tools for hacking and online sabotage : 1.6 billion USD
- ransoms obtained from use of ransomware : 1 billion USD

... and so on.

Digital Identity: A Serious Problem Still Unresolved

To date, there exists no *universal* digital equivalent of the passport. Trying to prove your identity online is impossible because—and this cannot be repeated enough—the libertarian "configuring powers" of the net have staked everything on connectivity and communication, with no concern for security. Fluidity is the key! The rest? Look at that later. Maybe. In the physical world, authentication of ID relies on direct cognition (meeting a person) or recognition (acceptance of ID credentials). But it is not so straightforward in the digital world. What happens in the case of lost, falsified, or stolen original documents? How about those famous "security questions" (mother's maiden name, and so on)? According to Google, the answers have been forgotten in 74 percent of cases. In practice, no technology currently meets all the necessary criteria of being simple, clear, unbreakable, and compatible with all user systems, computers, and smartphone platforms.

In the United States, a survey from November 2017 into the targets of cybercrime (*Javelin Identity Fraud Report,* March 2018) showed that 6.6 percent of American consumers had recently fallen victim to identity fraud, a rise of 8 percent on 2016. Total damages of identity fraud perpetrated against all internet users (including theft, fraud, compensation, replacement purchases and so on) amounted to 16.8 billion dollars.

In the United Kingdom, known cases of online identity fraud have exploded, increasing by 175 percent in the ten years since 2007, to a total of 175,000 in 2017.

Weaknesses: The Forgotten Human Factor

Fixated on the measurable, and with their screening and their high-level clearance rules spreading like wildfire, Washington has forgotten the crucial human factor. This much is clear from the inquiry into the theft of the NSA's secret cyber weapons, which reveals the damage done by an agency employee, a heavy-drinking mythomaniac who, over a number of years, "borrowed" an extraordinary quantity of secret files from TAO (see above). Measured in bytes, he had taken five times the volume of ALL the works in the Library of Congress—the biggest in the world. Documents were subsequently retrieved from hard disks found in the glove box of his car (which he drove while drunk) and in the shed at the end of his garden. For governments and businesses, the human factor plays a part in 28 percent of attacks (2016 data). It is humans who cover up IT security incidents, who mastermind phishing and malevolent social engineering attacks. And it is poorly trained, negligent, or corrupt staff (known to criminologists as "rogue technicians") who facilitate cyberattacks.

The Huge Outbreak of Hacking on the Omnipresent Cell Phone

Hundreds of security faults and malware are being discovered all the time in the Android system. After a lightning incursion, the owner loses control of their cell and therefore of their bank and cryptocurrency accounts. These are emptied by the hacker, who may also find compromising information or intimate photos with which to squeeze blackmail money out of the victim.

Spectacular Recent Hacks

EQUIFAX: a credit and financial management company with around 840 million customers around the world, of whom 91 million are businesses. In 2017, around 150 million customer dossiers were hacked: names, financial referents, address, date of birth, passwords, security questions, *all* of their financial details, and so on.

YAHOO: *all* of Yahoo's three billion email accounts were hacked.

US SECURITIES AND EXCHANGE COMMISSION: millions of the powerful stock exchange regulator's confidential emails were hacked, allowing subsequent

fraudulent manipulation of prices via insider dealing.

DELOITTE: one of the Big Four legal and financial consultancies, offering advice to clients on hacking, was itself hacked, with around 5 million emails stolen.

VINGCARD: this company supplies electronic locks and keys to tens of thousands of hotels around the world, involving millions of hotel rooms. Its system was hacked, though nobody seems to know to what extent.

The Risks and Dangers of Cryptocurrencies

This is not a retelling of the history of digital currencies, nor is it an explanation of the technology on which they rely. Rather, it is an attempt to show how, and how quickly, the most wonderful inventions of cyberspace have been put to criminal use. First, a reminder: these cryptocurrencies are neither secure nor regulated. Transactions carried out in Bitcoin, Ethereum, Ripple, Monero, Zcash, Dash, and so on, are untraceable and irreversible.

Crypto-yo-yo

What are these digital currencies "worth"? Strictly speaking, they are worth what the market dictates, from vertiginous highs to unfathomable lows. At the time of its first listing on August 16, 2010, a Bitcoin was "worth" 0.07 US cents. On December 17, 2017, that same Bitcoin was "worth" 20,000 dollars, and at the end of December 2017, the "Bitcoin bubble" was "worth" 140 billion dollars, equivalent to the market capitalization of the Coca-Cola Company. By the end of June 2018, a Bitcoin was "worth" 6,500 dollars—a 53 percent drop from January to June 2018. This roller-coaster ride can of course be explained by a range of geopolitical crises. But two kinds of criminal factor are also involved:

- hackers are particularly drawn to these fragile cryptocurrency exchange platforms. This is in direct contrast to systems based on Blockchain (a "secure technology with no central point of control, used to store and share data"). Blockchain is unbreakable.

- these cryptocurrencies are notorious as a tool used by criminals to handle ransom monies, money laundering, settle drug payments, and so on.

Hackers Target Cryptocurrency Exchange Platforms

- Since their beginnings up until March 2015, one in three Bitcoin exchange platforms were hacked. Half of those hacked subsequently closed.

- Between 2010 and 2016, 4 billion dollars were stolen by hackers from cryptocurrency platforms. More recent examples include:

- December 2017: NiceHash Bitcoin mining cooperative, possibly Slovenian, was hacked and lost 80 million US dollars' worth of cryptocurrencies.

- January 2018: Japanese platform Coincheck is hacked, losing 530 million dollars in cryptocurrencies.

- June 2018: South Korean platform Coinrail is hacked, losing 37 million dollars in cryptocurrencies.

- end of June 2018: South Korean platform Bithumb (the sixth largest trader in the world in this field) is hacked, losing 27 million dollars in cryptocurrencies.

Cryptocurrencies: Laundering the Proceeds of Crime

According to Europol, some 100 billion euros derived from criminal activity are laundered every year in the European Union. Of this total, 4 percent (around 5.5 billion euros) corresponds to cryptocurrencies. The police are powerless when it comes to this type of laundering.

- The UK now has around one hundred ATMs connected to cryptocurrency exchange platforms, handling Bitcoin and other cryptocurrencies in much the same way as a normal cash dispensing machine. Each of these Bitcoin ATMs is used by between ten and twenty customers a day, and according to one survey, 80 percent of them were drug dealers or speculators—or both. The shopkeepers who manage these ATMs describe a parade of individuals (often teenagers) "reeking of drugs" (*Daily Mail,* December 4, 2017) carrying out multiple transactions of 10-15,000 pounds sterling using wads of fifty-pound notes.

- Japan's largest yakuza syndicate, the Yamaguchi-Gumi, laundered around 270 million dollars between 2016 and 2018, via multiple small payments in Monero, Zcash, and others. Even so, this is only a tiny fraction of the yakuzas' turnover, which is estimated at 6 billion dollars a year, mostly derived from trafficking synthetic drugs, usury, real estate fraud, stock market scams, and so on.

- Colombian drug gangs with expertise in high-tech money-laundering have been using a Finnish Bitcoin platform to send home millions of euros made from the sale of cocaine in the European Union. This money transfer system is sufficiently sophisticated to enable the euros to be converted to Colombian pesos and then forwarded from Europe to banks in Bogotá in little more than twenty-four hours.

France: The Current Digital Threat

A number of sources provide information on the state of cybercrime in France. Despite their varied study populations and calculation methods, a dominant theme emerges: that France has not been spared by the cyber predators—far from it. The three countries most affected by cybercrime are, in order, the United States, France, and Russia. And the situation appears to be getting worse.

- In 2017, the INHESJ and the ONDRP[3] published the results of a survey they had carried out in France on quality of life and security. Using 2016 data on victims of crime and perceptions regarding matters of security, it showed that the number of victims of fraudulent payments from bank accounts rose from approximately 500,000 in 2010 (1.8 percent of the population) to around 1.21 million victims (4.3 percent of the population) in 2016. Thirty-four percent of these fraudulent payments were for less than 100 euros, while eighteen percent were for more than 1000 euros.

- In 2017, DEMISC,[4] which reports to the gendarmerie, amassed 63,500 files involving 320,000 victims, a 32 percent increase on 2016. These files concern every kind of problem relating to cyberspace and new information and communication technologies, including theft and fraud (67 percent of the total), identity fraud, use of ransomware, phone hacking, theft of personal data (email addresses, passwords, and banking security details), fake technical support rackets and a range of cyber incursions, child pornography, and glorification of terrorism.

Conclusion

Until cybersecurity engineers begin to understand the predatory nature of GAFA, their efforts—while tactically useful—will be as effective at the strategic level as taking a knife to a gunfight against a trigger-happy sadist, and the impact of cybersecurity will be little more than cosmetic. But calls for effective cybersecurity in an increasingly computerized and interconnected world are intensifying. Expert opinion underlines this:

> There is very definitely a demand, from people in many countries around the world, for a return to a shared order, to established

3 INHESJ: L'Institut national des hautes études de la sécurité et de la justice (French National Institute for Advanced Studies in Security and Justice). ONDRP: L'Observatoire national de la délinquance et des réponses pénales (French National Observatory on Crime and Criminal Justice).

4 DEMISC: Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (Ministerial Delegation to the Security Industries and the Fight against Cyberthreats).

> structures that could stem the far-reaching tide of recent change and bring back a degree of stability that the public now regard with a kind of nostalgia.(*Communication et Influence,* April 2018)

In the information society, the regulation of cyberspace must therefore be prioritized. But how can this be done? I propose the following diagnosis and treatment:

DIAGNOSIS: Cybercrime will not be reduced by the use of ever more high-tech solutions, but rather through political will. In matters relating to cyberspace, blindly rushing in wearing body armor, all guns blazing, would be even more disastrous than the inept high-tech war conducted in Iraq.

TREATMENT: Just as society responded to the age of the automobile by producing the rules of the road, so new rules for the information age must be created and imposed by a powerful global coalition—the countries of the G20, for example. Sooner or later, just such a normative digital superstructure will be put in place right around the globe. Just as the rules of the road apply to all vehicles, luxury and more modest models alike, so this digital rulebook will take aim at the internet titans, the crooked financiers, and the rest, who are currently plundering cyberspace and exploiting users with impunity.

Appendices

1 - Cybercrime, the key dates

[See *MalwareBytes, December 2017*]

1960s

- First cases of phone hacking (*Phone Phreaking*)
- "Val Smith" (an alias) falsifies data on a computer and embezzles money from his employer via false expense claims.

1970s

- (1976) Donn B. Parker publishes the book *Crime by Computer*.

1980s

- (1981) Ian Murphy, a.k.a. "Captain Zap", becomes the first hacker to be sentenced for hacking electronic billing systems at telecommunications company AT&T.
- (1986) The US passes its Computer Fraud and Abuse Act (CFAA).
- (1988) Early malicious software ("Morris Worm") infection released in the US. Its author, Robert Tappan Morris, is the first to be sentenced under the CFAA.

1990s

- (1990) In Los Angeles, Kevin Poulsen is arrested for hacking the phone lines of a local radio station in order to win radio phone-in prizes.
- (1994) A Russian hacker steals 10 million dollars from Citibank.
- (1996) Mathew Bevan and Richard Pryce commit the first (detected) large-scale hack of US military computers.

2000s

- (2000) The "Love Bug" virus from the Philippines infects 50 million computers in ten days, causing 5–8 billion dollars' worth of damage.
- (2000) First mass denial-of-service (DOS) attack launched by "Mafiaboy," causing eBay and Amazon to go down, at a cost of 1.7 billion dollars.

- (2003) Use of internet by consumers and business becomes widespread, and ordinary users are increasingly affected by spam and phishing.
- (2007) Massive DOS attack against Estonian government sites. Russian hackers suspected.

2010s

- (2010) The United States and Israel introduce the Stuxnet virus into Iran's nuclear systems.
- (2014) Sony Pictures suffers a massive hack carried out by "Guardians of Peace." North Korean hackers suspected.
- (2016): Suspected interference and manipulation in the US presidential election by Russian hackers.
- (2017) WannaCry and NotPetya ransomware attacks ravage the internet.

2 - Cybercrime: A Lucid Diagnosis from the European Parliament

[Extracts from the European Parliament's Report on the Fight against Cybercrime (European Parliament, July 25 2017)]

- ... the 2016 IOCTA [International Organised Crime Threat Assessment] reveals that cybercrime is increasing in intensity, complexity and magnitude, that reported cybercrime exceeds traditional crime in some EU countries, that it extends to other areas of crime, such as human trafficking, that the use of encryption and anonymization tools for criminal purposes is increasing and that ransomware attacks outnumber traditional malware threats such as trojans.
- ... there was an increase of 20 percent in the attacks on the Commission's servers in 2016 compared to 2015.
- ... devices connected to the Internet of Things (IoT), which include smart grids, connected fridges, cars, medical tools or aids, are often not as well protected as traditional internet devices and are thus an ideal target for cybercriminals ...
- the lines between cybercrime, cyber espionage, cyber warfare, cyber sabotage and cyber terrorism are becoming increasingly blurred; [...] cybercrimes can target individuals, public or private entities and cover a wide range of offences, including privacy breaches, child sexual abuse online, public incitement to violence and hatred, sabotage, espionage, financial crime and fraud, such as payment fraud, theft and identity theft as well as illegal system interference.
- ... a considerable number of cybercrimes remain unprosecuted and unpunished.
- ... growing links between terrorism and organized crime.

3 - Pinocchio Syndrome: The (Possibly) Enchanted Universe of the Start-Up

> Like so many other young cyber fans, Mathilde Ramadier found herself attracted to the idea of the start-up. But do the fruits do justice to the early promise? Hmm ...
>
> [Extracts from Ramadier's book *Bienvenue dans le nouveau monde: Comment j'ai survécu à la coolitude des start-ups* (Ramadier, 2017)]

"... The truth is that start-ups arm themselves with a veritable NewSpeak designed to disguise the law of the jungle in a cloud of cool. As with any language, it acts not only as a mechanism of inclusion, a tool of communication, it also rolls out a whole imagined universe around itself, creating new signifiers which help to construct a common frame of reference [...] but which can also make one believe in things that do not exist. In fact, behind the utopia sold by the start-up set, with its wealth of humanistic promises, hides an ultraliberalism that promotes ferocious competition and the pulverization of anything that appears even remotely stable [...]"

"[The managers are] super-quick, flexible, inexhaustible, perfectionists; these new buccaneers of the data age no longer serve either God or any Master; instead, they have but one word on their lips: innovation. The mere existence, even at a symbolic level, of their Mecca, Silicon Valley, acts as the mainstay of their sense of belonging to a project, a project henceforth referred to as the "family" [...] Set upon a fair and far-off pinnacle, Silicon Valley is constantly cited as an example, like a divinity that no one has ever seen. The dream it promises is, in fact, a nightmare [...]"

"After all, it is very reassuring to think that a revolution is under way in our turbulent times, and that kind and courageous young people are upending the established order so as to save us from everything that is dysfunctional about our society! Start-up NewSpeak ensures that the message spreads far and wide, enlisting the complicity of other actors, such as the state and a wide cross-section of the media [...] The solutions promised by the start-up set—a solution to the crisis, to unemployment, to boredom, to repetitiveness and obsolescence, to aging, to ugliness, and so on, are also built on a delusion: one cannot claim to already be living in the new world before it has actually been built. So, start-ups are "revolutionary" companies financed by "business angels," run by "rock stars," and fueled by "treasure hunters"? Hello!? Can we come back down to Earth for two minutes? The landing will be painful, I know."

4 – The Dark Web: A Catalog of the "Manufacture of the Weapons and Tools of Cybercrime"

[Extracts from Armor's *The Black Market Report: A Look Inside the Dark Web* (Armor, 2018)]

Monetizing hacking on the Dark Web: tools for sale, rates and prices, early 2018:

- Denial of service (DOS) tool for rent: 10 dollars per hour; 200 dollars per day.
- Basic hacking tool (Disdain Exploit Kit) for rent: 80 dollars per day; 500 dollars per week; 1,400 dollars per month; plus videos and courses on use and maintenance (or hacking work): from 100–150 dollars per month.
- Purchase of a "trojan licence": 3,000–5,000 dollars.
- A tool for hacking an online account: around 13 dollars; a tool for stealing passwords: 50 dollars.
- Denial-of-service attack (one week): 500–1,200 dollars.
- Tools for hacking cash ATMs: 700–1,500 dollars.
- Hacking tutorials: 5–50 dollars.

The Fake Payment Cards Market

- (each) Visa/MasterCard, United States: from 7-10 dollars; EU: 15–30 dollars.
- (each) American Express, United States: from 10-12 dollars; EU: 15–35 dollars.
- "Fullz" (payment card plus customized personal details the buyer needs to prove they are the card owner, top of the range):
- (each) Visa/MasterCard, United States: from 35-50 dollars; EU: 70–100 dollars.
- (each) American Express, United States: 35 dollars; EU: 70–100 dollars.

Market for Bank Account Information (or Similar), with Initial Balance

(Bank of America, JPMorgan Chase, Wells Fargo, PayPal):

- With 3,000 dollar opening balance: 300 dollars.
- With 20,000 dollar opening balance: 1,000+ dollars.

Identity Theft Market

Package including name and surname, address, phone number, social security number, bank account number, birth date, employment history, credit history, criminal history: 40–200 dollars.

Social Media Account Market

(Each): 13 dollars.

Hacked Instagram Accounts: (1,000) 15 dollars; (2,500) 25 dollars; (5,000) 40 dollars; (10, 000) 60 dollars.

Hacked Loyalty Card Market

- Airline miles account (United States): 1 account, 50,000 miles, 100 dollars; 100,000 miles, 150 dollars; 150,000 miles, 200 dollars.
- Airline miles account (Europe): 1 account, 25,000 miles, 35 dollars; 100,000 miles, 90 dollars; 150,000 miles, 120 dollars.
- Hotel chain rewards point account: 50,000 points, 75 dollars; 150,000 points, 140 dollars.

Reference List

Press, websites, and media, listed in chronological order starting with the most recent

New York Times International. August 4, 2018. "Rise of Tech's Mega Companies."

New York Times International. July 6, 2018. "To Hackers, We're Bambi in the Woods."

Les Numériques. June 21, 2018. "Marché des cryptomonnaies: la fin des illusions? Dévissages et piratages en série."

Le Figaro. June 20, 2018. "Les cybermenaces deviennent un phénomène de masse en France."

Les Echos. June 20, 2018. "Cette nuit en Asie: nouvelle alerte sur le Bitcoin après le braquage de la plateforme coréenne Bithumb."

National Public Radio. June 19, 2018. "Journalist Warns Cyber Attacks Present 'a Perfect Weapon' against Global Order."

Dark Reading. June 14, 2018. "Four Faces of Fraud: Identity, 'Fake' Identity, Ransomware and Digital."

BFM. June 11, 2018. "Le Bitcoin retombe sous les 7 000 dollars après un nouveau braquage."

BBC News. June 7, 2018. "Ship Hack 'Risks Chaos in English Channel.'"

Le Monde – June 5, 2018 - "La DGSI muscle ses capacités d'enquête 'cyber.'"

RT. June 3, 2018. "World Saw 'Worst Year Ever' for Data Breaches and Cyber Attacks in 2017 – Report."

Dark Reading. June 1, 2018. "Cybercrime is Skyrocketing as the World Goes Digital."

CBS News. May 20, 2018. "Was the Media Duped by Elizabeth Holmes?"

The Register (UK). May 17, 2018. "Biometrics: Better Than Your Mother's Maiden Name - Good Luck Changing Your Body If Your Info Is Stolen."

BTC Manager. May 16, 2018. "Japan's Biggest Newspaper Reports 30 Billion Yen Was Laundered Through Crypto Exchanges."

Reuters. May 11, 2018. "Apple is Almost a $ 1 Trillion Company, But Watch Out for Amazon."

Voice of America. May 11, 2018. "National Security Division Focuses on Combating Cyber Threats."

New York Times International. April 28, 2018. (Photo of Facebook Headquarters, Menlo Park, California)

New York Times International. April 21, 2018. "Silicon Valley and the Pentagon."

Europol. April 9, 2018. "Illegal Network used Cryptocurrencies and Credit Cards to Launder More Than €8 Million from Drug Trafficking."

Rolling Stone. April 3, 2018. "Can We be Saved from Facebook?"

Communication et Influence. April 2018. "Olivier Kempf "Guerre informationnelle et jeux d'influence dans le cyberespace."

New York Times International. March 16, 2018. "Cyber Attack on Saudi Plant had Deadly Goal."

Business Insider. February 12, 2018. "Criminals in Europe are Laundering $5.5 Billion of Illegal Cash through Crypto Currency, According to Europol."

New York Times International. February 12, 2018. "A.I. Picking up Some Biases from the Real World."

CBS News. February 10, 2018. "Brotopia Explores the Roots of Silicon Valley's Sexism Problem."

Computer Business Review. January 25, 2018. "Cybercrime Statistics: Hackers Still Having an 'Online Fraud Frenzy.'"

New York Times International. January 23, 2018. "Seeking an Elusive Cure for Cyber Attacks."

New York Review of Books. January 18, 2018. "Bitcoin Mania."

Daily Mail. January 12, 2018. "Elon Musk Reveals he Attended a 'Drug-Fueled Silicon Valley Sex Party' at an Investor's Home, But Insists He Left Early and Thought

It Was Only a 'Costume-Themed' Gathering."

Vanity Fair. January 2, 2018. "Oh My God, It's So Fucked Up - Inside Silicon Valley's Secretive Orgiastic Dark Side."

MalwareBytes. December 2017. "Une brève histoire du cybercrime."

Daily Mail. December 4, 2017. "Teenagers Reeking of Drugs Deposit Wads of £50 notes in Bitcoin Cash Points."

New York Times International. November 15, 2017. "Leaks Shake Agency to Its Core."

Financial Times. October 30, 2017. "Washington Appears to Have Fallen Out of Love with Silicon Valley."

New York Times International. October 20, 2017. "Vision of a World According to Google."

New York Times International. October 18, 2017 - "Silicon Valley is Not Your Friend."

New York Times International. October 17, 2017. "North Korea Wreaks Havoc with Its Corps of Hackers."

New York Times International. September 8, 2017. "Tech Giants, Liberal but With a Twist."

New York Times International. September 6, 2017. "In Silicon Valley, 9 to 5 is for Losers."

Security Defense Business Review. September 5, 2017. "La menace dans le cybermonde de 2017."

New York Times International. August 23, 2017. "Phone Numbers Let Hackers into Wallets."

New York Review of Books. August 22, 2016. "They Have, Right Now, Another You."

Books – listed in chronological order starting with the most recent

Establier, Alain, and Xavier Raufer. 2018. *Cybermonde et nouvelles menaces: La cyber-sécurité par ses principaux experts*. Boulogne-Billancourt: MA Editions.

Ramadier, Mathilde. 2017. *Bienvenue dans le nouveau monde - comment j'ai survécu à la coolitude des startups*. Paris: Premier Parallèle.

Levieux, François, and Eric Meillan. 2017. *Survivre à la guerre numérique*. Paris: Picollec.

Raufer, Xavier. 2015. Cyber-criminologie. Paris: CNRS Editions.

Heidegger, Martin, and Eugen Fink. 1979. *Heraclitus Seminar 1966/67*. Translated by Charles H. Seibert. Alabama: University of Alabama Press.

Marx, Karl, and Friedrich Engels. 1968 [1846]. *A Critique of the German Ideology.* Moscow: Progress Publishers. Available at: https://www.marxists.org/archive/marx/works/1845/german-ideology/ch01b.htm.

Reports - listed in chronological order starting with the most recent

European Parliament. July 25, 2017. *Report on the Fight against Cybercrime*.

Armor. March 2018. *The Black Market Report: A Look Inside the Dark Web*. Available at: https://www.armor.com/webinars/black-market-report/.

Revue Stratégique de cyberdéfense. February 2018. Available at: http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

Strategic Review of Cyberdefense. February 2018. (English Overview of the *Revue Stratégique de cyberdéfense*). Available at: http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf).

Javelin Identity Fraud Report. March 2018. "Survey Data Collection." Available at: https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity.