

Narrative Mapping of Cyberspace. Context and Consequences

David Harries

Abstract Cyberspace is barely two decades old. Yet it is already globally pervasive, powerfully disrupting perceptions and realities in the legacy spaces; on the land, at sea and in the air where human beings live, move and work. The pace at which its influence is spreading and intensifying is amazing; the number and reach of the consequences arguably even more so, and they continue to emerge, mash-up and surprise. For humanity and its planet, an acceptable future depends on ‘seeing’ and understanding Cyberspace well enough to do two things; manage and exploit it successfully in the present, and make timely, flexible preparations for a future that is uncertain, except in that it will be different to today, in no small part because it will be substantially shaped by the state of and actions in the Cyberspace. This chapter is a first attempt to explain why Cyberspace has become so important so quickly and describe briefly the most meaningful of its initial consequences, all with the aim to promote strengthening the good in Cyberspace while keeping the bad in check.

Keywords Context • Consequences • Borderlessness • Vulnerability

1 Introduction

Mapping ‘the Cyberspace’ calls, arguably, for three distinct but related maps. Each one needs a legend or key. One map is of Cyberspace structures and processes. Put in the simplest terms this map answers the question; What is the Internet? A second map shows what is taking place—what is being done—in Cyberspace. The third

Submitted: 4.10.16; Accepted: 3.11.2016.

D. Harries (✉)

Chair Canadian Pugwash Movement, International Practitioner of Security Foresight,
Kingston, Canada

e-mail: jdsharries@bell.net

map is of the context in which Cyberspace exists, its activities take place, and their consequences play out. It is a ‘motion’ picture of trends and drivers of cyberspace’s character and consequences in an increasingly connected, but uneven, world.

The legends for these maps are works in progress, for three main reasons. First, the Cyberspace is young; barely out of its teens. Social media, arguably the most globally influential element of Cyberspace, is even younger. Second, it exists in a world stressed by accelerating, often shocking, change. And, third, Cyberspace is a self-organizing intangible that defies proactive control.

All three legends need to cater for the scope, spread and significance of Internet activities, which are encouraged most strongly by the technology imperative (Buzan 1987). Any legend for a map of Cyberspace context calls for metrics and pictures that depict matters as grand as globalization and as granular as the well-being of individuals. For this reason, it was decided to focus, narratively, on the context and consequences of Cyberspace; what is obvious today and what can be foreseen for plausible futures.

This chapter attempts to explain how and why a ‘space’ that only recently came into existence has so quickly become so pervasive and so powerfully disrupted perceptions and realities for the legacy spaces; land, sea and air, of human existence; of living, moving and working. The explanation is incomplete, and will remain so until a number of questions can be answered in more detail than is possible today. Finding useful and appropriate answers, and identifying the important connections and overlaps among them, will be challenging given Cyberspace’s ephemeral and ever-changing nature.

This fact leads to the author to conclude that more time and effort needs to be routinely devoted to Cyberspace Foresight. The Cyberspace became globally important very quickly, and the pace at which its influence is spreading and intensifying is amazing. For humanity and its planet, an acceptable future depends on ‘seeing’ and understanding Cyberspace well enough to do two things; manage and exploit it successfully in the present, and make timely, flexible preparations for a future that is uncertain, except in that it will be different to today, in no small part because it will be substantially shaped by the state of and actions in the Cyberspace.

2 Cyberspace Context

2.1 Context Background

In 1984 William Gibson, who coined the term ‘cyberspace’ on 1982, published his novel *Neuromancer*. It tells the story of a washed-up computer expert hired by a mysterious employer to pull off the ultimate hack. *Neuromancer* is the name of one of two Artificial Intelligence characters in the story, both of whom would be at home in 2016.

Until, arguably, the 1990s, if someone, say a whistle-blower, wanted to tell another person something ‘privately’, without others knowing about or seeing the

message, the ‘brown envelop’ was standard practice. If the information needed to be sent to many people, copies had to be made, and individual envelopes addressed. Today, ‘snail mail’ whistle-blowing is rare,¹ not only because it is so slow, but because a message can now be sent to any number of others, in the Cyberspace, in less time than it takes to manually address one envelope. In addition, the sender can choose from a variety of Cyberspace ways and means to remain anonymous.

The Cover Story of the June 2011 Consumer Reports magazine was titled ‘Your Security’. The first three articles were: (1) 25 things cops and crooks say you have been doing wrong, (2) Why your accounts are vulnerable to thieves, and (3) Door locks; all conventional information and advice seen well before 2011 and little changed, except for updating technology and cost factors for 2011. The *fourth* and last article in the package was: ‘Online Exposure: Social networks, mobile phones and scams can threaten your security’. The list of ‘details’, highly focused on ‘abuses’ on Facebook and careless mobile phone use, ended with the statement: “The persistence of Internet threats makes it important to use security software. In our tests we found that free anti-malware programs should provide adequate protection for many people.” The next article in the magazine was a seven-page Report: Portable Computers The new choice: tablet, laptop, or netbook. Not once does the word ‘security’ appear.

The Special Report of the July 12th 2014 edition of The Economist, was titled Cyber-Security: Defending the digital frontier, begins with a reference to William Gibson’s coining of ‘cyberspace’. It highlights the paradox that, on the one hand the internet has “...brought tremendous benefits to everybody who uses the web...” and on the other that “there is a darker side this extraordinary invention”, in terms of all of commerce, national security, public safety, conflict and recourse for abuse. The 14 page narrative is virtually all about the ‘darker side’ of the Internet, and on people’s willful blindness to its Janus-like nature; the threats and the opportunities of weak source codes, hacking, exploding, unconstrained and unpredictable connectivity, negative externalities, cyber-crime and cyber-extremism, and plausible deniability. Nothing in this 2014 Report needs to be changed for 2017 except, maybe, its closing message; Prevention is better than cure, which is outdated. ‘Defending the digital frontier’ can no longer be done only, or best, by prevention. As soldiers know, and as the growing community of commercial and state-sponsored organizations have taken to heart, offence is the best defence.

Today, it is a rare for newspaper or newsmagazine not to have something on the status, security or activities in Cyberspace, so embedded, so ‘normal’, has it become in everyday life, world-wide.

¹Rare, but not never. Parts of Donald Trump’s 1995 tax returns were mailed in August 2016 to a NYT reporter. See http://www.nytimes.com/2016/10/02/us/politics/donald-trump-taxes.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=b-lede-package-region®ion=top-news&WT.nav=top-news&_r=0.

2.2 *Contemporary Context*

The arrival of the Cyberspace offers unprecedented power to individuals and organization that, beforehand, could neither attain nor exercise it. Today, everyone with an internet connection has significant power. The most powerful are those who first place ‘information’ in Cyberspace. If the information is ‘true’, those who first exploit it in productive ways can become a more powerful competitor in their field. Information that is not ‘true’ can both engender power, and weaken it. Its receipt weakens the relative power of those who do not know it is false information, the more so if they use it in the belief that it is true. Recipients who know the information is false have a choice. On the one hand, they may see it as a threat to their reputation or resources that demands the time and effort (power) to immediately rebut or correct it. On the other hand, if the untrue information is not a threat to one’s current well-being and intentions, the falsehood may represent nascent power that can be used in the future, possibly against its sender.

There are many choices for the name of the ‘age’ ushered in by the arrival of the Cyberspace: the digital age, the information age, the internet age, the computer age, the connected age, the Google age, the emoji age, the cloud age, the smartphone age, the data age, the Facebook age, the robot age, the post human age (Aeon 2016). The more names it is given, the more vaporous it seems, but whatever age has arrived, it is definitely one of information and data glut. The glut is growing exponentially as more people and organizations use systems and servers that are becoming faster, and smarter. It has become possible to find in Cyberspace masses of material on virtually any subject, in tiny fractions of a second.

However, reading and filtering all that can be found, to identify the parts that can be used or that need defending against grows ever more humanly challenging. Evidence of this fact is a recent Aeon report:

Since 2010 Twitter has been providing the library with every tweet that’s been posted publicly. It was supposed to be an archive for researchers. Managing that massive data dump, however, has proven to be a challenge the library has no idea how to handle it (McGill 2016).

The situation is a prime driver of development and deployment of faster and smarter Cyberspace tools. The number of individuals and organizations both active in Cyberspace and keenly aware how empowering their engagement can be, also is rising exponentially. The rise is self-reinforcing/self-sustaining. It is human nature to not want to be behind, or to be left out, or to risk being ignorant, and especially to be so described. Cyberspace has spawned a new metric for the old mantra ‘keeping up with the Jones’.

Virtually everywhere on earth is under stress. There may be a few humans who are calm and have valid reasons to be so, but the great majority are, depending on the time and their circumstances, one or more of concerned, challenged, fearful, threatened, under attack, flailing, failing, defeated, or victorious (for reasons both real and perceived). The variety of the causes, degrees, validity, longevity and durability of stress, and of the response to it, has left the human condition massively

uneven globally, arguably more uneven than at any time in human history and becoming ever more so. The manifestations of the unevenness, whether in terms of freedom, equality, stability or security are, thanks greatly to the Cyberspace, ‘open source’ information in real-time.

Globalization has effectively ended the ‘sovereignty’ of the infrastructure of each nation. The merit, value and integrity of infrastructure in one state, even the built parts, are no longer best measured primarily by and in that state, but in terms of the costs and the benefits relative to and shared with other states. Even the most powerful and richest states can no longer claim to be truly self-sufficient. Global supply, distribution and transportation chains, global wicked problems such as climate change, global monies (bitcoin) and money-moving (blockchains), and the global Cyberspace in which all are engaged and enabled, have relegated national self-sufficiency to the status of at best an occasional, temporary strength, and at worst an historical concept still governing national policy.

Extremism is a global phenomenon that appears in many forms and plays out in many fields. Cyberspace is where virtually all extremists market, demonstrate, contest and preach. One extremist’s statement or action can be globally known in seconds. Since there is no recall or removal from (somewhere in) Cyberspace, the message or picture becomes one of an ever increasing mountain—glut—of eternal facts. In technology’s distant past, it was sometimes possible to erase or silence news of a fact or event that those with necessary power and authority to do so did not want to become public knowledge. Today, even the most undemocratic countries, ones that go to extremes to stop their people from knowing about others, or the outside, can no longer totally seal their borders. The borders that Cyberspace recognizes are different to and usually at odds with the borders on the maps used by states and all other actors for whom ‘international’ retains a tangible meaning.

Long ago, crime and punishment were local, clearly defined and directly related. Over time, laws, the authority to monitor and enforce them, and justice, became more complicated and complex. Today they are ambiguous and incomplete, in large part because they have failed to keep pace with globalization dynamics. No law exists today that applies world-wide, or to all of any of the many recognized regions, or to the geopolitical stew of states, para-states, non-states and pseudo-states. Public organizations, nonpublic organizations, private individuals and corporate actors are all different in legal terms, even if in the same state. In addition, laws that apply to some of them may conflict with some that apply to others. There is no global body with the mandate to harmonize even the most costly and damaging of those contradictions. ‘Law’ is still made very much as it was in the 19th century, but governments from the very best to the very worst are all exploiting Cyberspace to promote their interests of the day.

Unsurprisingly, dictatorships are more effective at making laws, dealing with crime and meting out punishment in these times of context compression, than are democracies. The latter, even those using the internet in enlightened ways, are slowed and obstructed by democratic standards and practices from fully exploiting Cyberspace characteristics. This inherent power-lessness is intensified by the ‘information glut’ referred to earlier. The ever-increasing mass of necessarily relevant

information deserves ‘fair’ and full—i.e., democratic, review by all stakeholders before a decision is made about a law or a punishment. Widening gaps in relevance and content among laws, regulations and standards are further delay legal process and judgement, leaving democratic governments ever more stressed by the tensions between fairness and justice.

The small world—that Cyberspace and technology have co-provoked—is growing more and more crowded, not only with people but with barriers. More ‘silos’, filters and barriers—physical and virtual—are being erected or re-erected. In part this is a reflection of the unhappy state of the world’s geopolitics and of security fragmentation. Each silo, filter or barrier takes up space that cannot then be a ‘commons’ where people can live, move or work freely and productively. The increase in barriers is due to one or more of misunderstandings, inappropriate biases and assumptions, selfish interests, real and perceived fears of weaknesses in national security and public safety, context incompetence, and survival uncertainty. The barriers have many forms, among them; physical walls, trade protectionism, censorship, surveillance, ethnicity, education, and religion. The more barriers that go up, the more effort and resources that are deployed to monitor and defend them, and the less ‘openness’, equality and opportunities there are for more and more people. The inevitable result; and the more so as activities in Cyberspace highlight the trend, is greater likelihood of significant and substantive differences among individuals and peoples as space to live, move and work free from fear and want shrinks.

On land, crowding is being provoked by an even more pervasive trend; the continuing increase in the number of sovereign states, each of which insists on borders on maps, their side of which they control. New borders reduce the space for ‘commons’. The global mantra of entitlement to self-determination and independence reinforces the growth in physical borders as several to many more of the thousands of nations aspiring to statehood feel justified in doing so. How many of them will succeed in joining the 193/200 existing states, and when in relation to population growth now estimated to be heading to 11 billion, or more.

3 Cyberspace Consequences—General

The ‘arrival’ of cyberspace has already meant lives the majority of human beings has a ‘family’ of new, changed and changing challenges—both threats to be faced and opportunities to be seized—in the traditional spaces where everyone lives, moves and works. How bad are the threats and how good are the opportunities will be determined by an unpredictable, and unmeasurable combination of our proaction for and our reaction to them.

Cyberspace needs regulation. Considerations of who, how, and at what cost management, regulation and control can be established have barely begun. But, until they are effectively in place, individually and collectively, identifying, deploying and governing the effort to deal with the planet’s existing, and arguably

intensifying ‘wicked problems’; among them Climate Change, Conflict and Context Compression may be more confusing than constructive.

Any map of consequences of the CS and its activities will show a living, self-organizing mash-up of what first and early on were seen as almost universally positive and bright impacts, and the increasingly more numerous less positive and darker pictures as its activities reached ever more deeply into ever more aspects of human life. The whole map is blurry, with little in focus even in the short periods between events and circumstance changes that redraw, recolor and reorient its features. Grey spaces on the map signal that there is still more to be learned about consequences provoked in the short Cyberspace past. Dark spaces unknown unknowns, and will be where the inevitable wild cards and black swans substantially and suddenly—in an artistic explosion—disrupt all or most of the map because not enough was known to put in place the ways and means to soften the blows.

4 Overarching Consequences of Cyberspace

In these early years of the Cyberspace, in a world where the *status quo* is shocked and disrupted with alarming regularity, and given that the writer is not a cyberspace expert, it borders on the presumptuous to claim that the following are, already, overarching, or permanent, consequences. However, even if they prove less august with time, they *will* feature on any map of the Cyberspace.

1. First, and foremost, anyone who is connected to the WWW, or whose lives depend on goods or services connected to it, is potentially vulnerable to any and all of the threats from the dark side of the internet. The more frequent the connection, and the ‘smarter’ the goods and services and the more connections among them, the greater the vulnerability.
2. What the Cyberspace provides; universal and enduring visibility of all in it, provides people with ever more ‘knowledge’—true and false—about their concerns and fears and the challenges and threats facing them. This intensifies their already high levels of stress. Rising stress is promoting greater unevenness of the human condition globally, and reinforcing the trend—also apparently global—of rising numbers with mental health problems, primary among them being PTSD and abject desperation. The former was formally recognized only a few years before the Internet arrived, primarily as a soldier’s mental health issue. Today, thanks to the Internet’s ability to show everyone the most horrific things in near real time, and medical progress, virtually everyone has become a ‘first responder’—if only mentally—to the evils of our times. Abject desperation is driving more people to risk all to improve prospects of survival with freedom, and others to see no alternative but to buy into extremists’ ideologies, usually imposing conditions that are anything but free, and calling for behavior that precludes survival.

As Nicholas Carr writes “Technology promised to set us free. Instead it has trained us to withdraw from the world into distraction and dependency.” (Carr 2016; Weintraub 2016).

3. ‘The truth, the whole truth and nothing but the truth’. Long the standard for participation in processes to assess right and wrong and judge on the findings, this call has, in whole, become an impossible task. Veracity has been recontextualized to be a reflection of only what is known and being considered at a given place and moment in time. It has become a vision in search for more and better truth. The age of truthiness has arrived, an imperfect age both governed and driven by the only contemporary ‘truth’; uncertainty.
4. The WWW both draws people together and drives them apart. Its contents can shift the relationship from positive to negative in the time it takes to read the latest email. Scanning the web, depending on one’s reason (Harries 2016) for doing so, quickly demonstrates that there is more than enough evidence, opinion or speculation in Cyberspace to allow even the most rational of scanners to come off the fence on the side of either camp arguing about almost any issue.

5 Specific Consequences of Cyberspace: A Selection of Four

The consequences of the Cyberspace will continue to grow in number and therefore in their influence on everyday life. The positive ‘good’ ones are much discussed and generally agreed. However, negative ‘bad’ consequences receive less than their due, including accounting for the fact that many and arguably most Cyberspace consequences should be seen as offering a set of good and bad ones. The main problem in differentiating the two can be expressed by a paraphrase of a familiar statement: One man’s terrorist (bad consequence) is another man’s freedom fighter (good consequence).

Mr. Snowden has seen significant success in his quest to start a public conversation about government surveillance. In 2015, the N.S.A.’s bulk collection of Americans’ phone records, one of the programs he exposed, was ruled illegal and transformed by Congress. He has also won widespread support abroad, including from the European Parliament, which adopted a nonbinding resolution in October to protect him from prosecution and recognize him as a “whistle-blower and international human rights defender” (NYT 2016a).

This problem is exaggerated by all four of the overarching consequences briefly described above: Vulnerability, Stress, Truthiness, and IFF (identifying friend or foe), in large part because all are ‘in motion’; sensitive to time and circumstance and inherent opaqueness.

Five consequence fields have been selected for brief, and therefore far from deserving, attention; Power, Conflict, Personal Well-being, Business, and Foresight. There are myriad, dynamic connections, overlaps, and influences among them, but doing that fact justice would demand a map with detail and fineness that

is beyond the scope of this paper and the ability of the author. The fifth field; Foresight, is chosen not only because it one the author knows and practices, but to introduce the concluding section of this think-piece; a set of Questions whose full or partial answers will increase the likelihood that consequences of the Cyberspace now, those emerging, and those shaping and in the future, can be identified and understood in time to be appropriately managed.

The focus is on the ‘bad’, or at best the less good consequences, as these are invariably the ones demanding the most attention, soonest.

5.1 *Power Consequences*

Information is power? Information is power if it is used. For the first time in history a single individual can hold a nation or group of nations hostage to an uncertainty, or threaten or attack them in both tangible and intangible ways. Even a nuclear threat or an attack which—other than in the tragi-comical rants of the North Korean dictator—have not featured in internet exchanges, calls for the deliberate participation of several persons and substantial resources.

But it remains impossible to know with absolute certainty if an event in Cyberspace is the act of an individual, or of an organization, or of a state, or of a group of states, unless the actor confesses. Organizations and states rarely confess, even when caught. Individuals do; the most famous being Manning, Assange and Snowden, some even when not caught. In any case, plausible deniability exercised smartly offers any attacker more ‘power’ to deploy uncertainty.

Who or what is Guccifer 2.0? Who or what is? are? the Illuminati? Uncertainty has been enriched by the wholesale writing of history globally, an activity given wings by the Cyberspace where everyone can become an historian, not only as before the internet, only the victors or the rich and powerful with the wherewithal and discretionary time to put pen to paper and attract publishers. The many new histories have severely dented the reputation and therefore the power of all who, in the present, rose to power on the back of traditional, but incomplete or half-truths or outright falsehoods. The power of the new historians and of the communities their news spawns is already significant enough to counteract traditional state-based strengths (NYT 2016b).

The strong are now less powerful if they do not exploit the Cyberspace. Putin, the forceful leader of a huge country that is actively deploying cyber weapons, no doubt in part to make up for the host of problems; economic, social, political and military that are weakening Russia (Tsygankov 2016).

“Using both conventional media and covert channels, the Kremlin relies on disinformation to create doubt, fear and discord in Europe and the United States (MacFarquhar 2016)”.

But exploiting the Cyberspace has its downsides, and raised many unprecedented questions that do not have durable answers. Even if officials of the US—far and away the most militarily powerful and globally deployed nation in

history—obtain proof of who or what has used a Cyber tool or weapon to attack the country, or lied to them, or stolen from them:

they may not be able to make their evidence public without tipping off Russia, or its proxies in cyberspace, about how deeply the National Security Agency has penetrated that country's networks. And designing a response that will send a clear message, without prompting escalation or undermining efforts to work with Russia in places like Syria, where Russia is simultaneously an adversary and a partner, is even harder (NYT 2016c).

Again, on Guccifer 2.0 and the Illuminati? Who are their friends. Who are their enemies? Are the two always enemies?

5.2 *Consequences for Conflict*

Booby traps have been a weapon for centuries. The arrival of the Cyberspace allowed them to move on from what were historically manually produced, in-place, crudely timed and simply controlled (if at all), victim-activated weapons for defence and protection or psychological effect to become a far more fearsome weapon controlled by the attackers. Since 2001, more NATO deaths, casualties and PTSD have been attributed to the now infamous IED (Improvised Explosive Device), often wirelessly controlled (RCIED), than to any other Taliban or warlord weapon (or to friendly fire accidents).

There are no principles of war for Cyberwar: “Mr. Obama often says the world of cyberconflict is still “the Wild West.” There are no treaties, no international laws, just a patchwork set of emerging “norms” of what constitutes acceptable behavior (NYT 2016c)”.

There are no norms for Cyberwar. Who admits what? Who is qualified (has the authority) and competent (the technical knowledge and skills) to speak? There are neither norms for evaluating cyber education and training, nor certifying those educated and trained. Does that mean anyone can be an expert?

Decisions on Cyberwar options are more guesswork than judgement. The situation is a duel of uncertain facts in a fog of uncertain second and third order consequences of unpredictable costs and benefits.

In the Democratic National Committee* case, two senior (US) administration officials spoke on the condition of anonymity to discuss the options, ranging from counter cyber-attacks on the F.S.B. and the G.R.U., two competing Russian spy agencies at the center of the current hacking, to economic, travel and other sanctions aimed at suspected perpetrators (NYT 2016d).

Way and means to exploit the Cyberspace to attack others; to disrupt, to destabilize, to destroy, to confuse, to discourage seem unlimited:

every new case (attack) brings a new and imaginative way to weaponize cyberpower. Until November 2014, when North Korea hacked into the computers at Sony Pictures Entertainment in retaliation for a comedy that portrayed a C.I.A. plot to assassinate Kim

Jong-un, the country's leader, no one seriously considered a movie studio to be "critical infrastructure." (NYT 2016d).

The United States is, by far, the world's most aggressive nation when it comes to cyberspying and cyberwarfare. The National Security Agency has been eavesdropping on foreign cities, politicians, elections and entire countries since it first turned on its receivers in 1952. Just as other countries, including Russia, attempt to do to the United States. What is new is a country leaking the intercepts back to the public of the target nation through a middleperson. Unlike the Defense Department's Pentagon, the headquarters of the cyberspies fills an entire secret city. Located in Fort Meade, Maryland, halfway between Washington and Baltimore, Maryland, NSA's headquarters consists of scores of heavily guarded buildings. The site even boasts its own police force and post office.

And it is about to grow considerably bigger, now that the NSA cyberspies have merged with the cyberwarriors of U.S. Cyber Command, which controls its own Cyber Army, Cyber Navy, Cyber Air Force and Cyber Marine Corps, all armed with state-of-the-art cyberweapons. In charge of it all is a four-star admiral, Michael S. Rogers.

"Cyber Command itself has always been branded in a sort of misleading way from its very inception, Snowden told me. It's an attack agency. ... It's all about computer-network attack and computer-network exploitation at Cyber Command" (Snowden 2014).

The idea is to turn the Internet from a worldwide web of information into a global battlefield for war. "The next major conflict will start in cyberspace," says one of the secret NSA documents. One key phrase within Cyber Command documents is "Information Dominance (NYT 2016d)".

NSA was, fairly certainly hacked in recent times. Officials and a 'former TAO operator' stridently responded to the news, that included an offer to auction more NSA data than had already been exposed, with emotion: 'the auction is a joke' and that the auctioneer 'doesn't have everything' (Nakashima 2016). True? False? How do they know?

War is becoming more and more automated (La Pointe and Levin 2016). Gone are the days of 'line of sight' battle, front lines, and soldiers fighting other soldiers. Indeed, it is only two decades since communications technology created the conditions for the appearance of strategic corporals and tactical generals, so visible had the whole battlefield become; visible, because of the deployment of drones. Then came drones with weapons, then bigger drones with more weapons and longer ranges and staying time. Generals in Florida and drone pilots in the center of the US fought the battle in Afghanistan. In 2012, the USAF trained more UAV pilots than ordinary jet fighter pilots for the first time. As observable data becomes even more granular and algorithms improve, autonomous systems will be able to support commander decisions.

In contrast to the famous Hellfire equipped Predator, which is remotely piloted via satellites, the Global Hawk operates virtually autonomously, and is leading the shift to the next level of war at a distance. Advances in AI are speeding the arrival

of all manner of autonomous armed robots. How autonomous these Cyberweapons can be (technology), will be (geopolitical decision), and should be (humanitarian and ethics concerns), are issues under intensifying scrutiny.

Asymmetrical warfare? ISIS in the Middle East is losing territory in Iraq and Syria, predominantly because US, and probably others' airstrikes are picking off its leadership and attacking important facilities and resources. ISIS therefore increasingly needs to "depend upon its "virtual planners"—members who operate in the dark spaces of the Internet—to inspire and coordinate attacks abroad" (Foreign Affairs 2016).

5.3 Consequences for Personal Well-Being (Human Security)

The Cyberspace has significantly complicated 'human security' and forced new metrics upon it. As willingness to acknowledge—see—the consequences of the Cyberspace and as understanding of them rises, the metrics are beginning to appear. Primary among them is a grudging rebalancing of the relative priorities of security and personal freedoms. There is a more realistic attitude toward electronic surveillance and its contested but unavoidable role in modern counterterrorism, and acceptance that 'liberty' will be less. This ever stronger reality particularly rankles Americans—remember the motto of the State of New Hampshire, on every vehicle license plate: "Live Free or Die"—but is making its mark much more widely.

Again from Carr:

Technology promised to set us free. Instead it has trained us to withdraw from the world into distraction and dependency. The culture that emerged on the network, and that now extends deep into our lives and psyches, is characterised by frenetic production and consumption—smartphones have made media machines of us all—but little real empowerment and even less reflectiveness. It's a culture of distraction and dependency (Carr 2016).

The Swiss have seen the 'writing on the wall':

The Swiss (recently) voted in favor of increased government surveillance. Fear of terror attacks trumped Switzerland's traditional wariness of government snooping. More than 65% of voters were in agreement with the law that gives the Federal Intelligence Service more power to tap phones, read emails, and use bugs and hidden cameras." (BBC 2016).

Privacy? Yahoo Says Hackers Stole Data on 500 Million Users in 2014 (Perloth 2016). To what end? What should the millions of owners of the hacked accounts do? Who is accountable? (Satter and Cheslow 2016). "The spyware took advantage of weaknesses in Apple's mobile operating system to take complete control of iOS devices (...) YouTube may be teaching someone to spy on you (Kasulis 2016)".

Confidentiality? WADA systems have been hacked. Given the intense and continuing war against doping in sports, the ends for the hacker may seem obvious, but what are the thousands of athletes whose tests' data is no longer confidential to do? Has any of the hacked data been tampered with? Are whistleblowers safe?

Confidential athlete medical data relating to last month's Rio Olympics has been hacked and published by a Russian cyber espionage group with the threat of more to come, the World Anti-Doping Agency (WADA) said. It identified the group as Tsar Team (APT28), also known as Fancy Bear. The www.fancybear.net website said it had information about a number of U.S. athletes, including tennis sisters Serena and Venus Williams as well as multiple gold medal-winning gymnast Simone Biles. WADA revealed last month that Russian whistleblower Yulia Stepanova's electronic account had been illegally accessed with a "perpetrator" obtaining details which would normally include her registered whereabouts (...) Personal safety and health? Stepanova, referred to in the previous paragraph, is in hiding in North America, having been forced to flee with her husband for fear of her life after helping reveal the biggest state-backed doping programme in Russia (Ruiz 2016).

Social Policy planning based on good data, reliably available?

"Australia has halted online collection of national census data after a website where citizens could upload information was subjected to repeated cyberattacks. The Australian Bureau of Statistics said its website had experienced four denial-of-service attacks, in which a torrent of automated requests is sent to overwhelm a site. The last attack, just after 7:30 p.m. on Tuesday, contributed to the overloading of a router, which led to the decision that night to close down online data gathering. The census, which occurs every five years, has been the subject of intense criticism and questions this year over whether the introduction of online data collection could leave Australians' personal information at risk (Ramzy 2016)".

Canada, a relatively safe and respected state, is increasingly challenged by Cyberspace to manage both global and national contexts in appropriate fashion (Bell 2016). Activists in Canada critical of Beijing have found themselves targets for intimidation. Notwithstanding the clarity of the situation, they apparently have no recourse—they are 'powerless'.

"Not long after Zang Xihong, 54, a prominent Chinese human-rights activist, emigrated to Canada 27 years ago, she said, she began receiving menacing phone calls from Chinese state security agents at her home in the Toronto suburbs. In recent years, she said, the harassment has grown more ominous. Her face and phone numbers have been digitally inserted into pornographic escort ads, she said; hackers have posted photos stolen from her computer; and articles have appeared online accusing her of embezzlement. She has also been sued by a man who claims she was responsible for his cousin's death in China. Zang said Canadian authorities had told her that they could take no action because most of those activities were protected free speech, leaving her powerless, she said, to escape the long arm of the Chinese government or its supporters (Waterloo Chronicle 2016)".

Buying and selling safely? "Another woman was also scammed by a man who matches pictures of Reid. Liat Feldman just moved back to Toronto after living overseas for 18 years. She says that she, too, was scammed out of \$1100 at the same apartment on the same weekend as Langton. "You can't go onto the internet anymore and find legitimate apartments," she told CBC. "You don't know who you can believe" (CBC News 2016)".

On “The Current” a highly respected current events programme provided weekdays by Canada’s national broadcaster, the CBC, the interviewee, who had just had his book published on the state of the global con game, remarked that the con business is exploding in Cyberspace, that there is little chance, and therefore fear of being caught, and therefore next to no fear of ever being punished (Tremonti 2016).

5.4 *Consequences for Business*

There are arguably three predominant consequences of Cyberspace for business; new business, new map and new players. A detailed analysis of the three and of others of importance is in preparation.

1. New business. The business of Cybersecurity business has changed. It was, in the beginning the somewhat esoteric activity of providing the goods and services to get on the internet and protect computers and their connectivity from viruses and malware and remove those that make it through, or that infected the internet resources of those who—for quite a number of years in large numbers—did not think it necessary to invest in protection. It then briefly moved to protection and identification of attackers. Quickly, with states or state-sponsored or authorized private organizations in the lead, it has achieved what can be termed war footing; active in overt and covert defensive and offensive and psychological operations with substantial geopolitical overtones.

For example, Mr. Obama has pressed President Xi Jinping of China to work with the United States and other nations to develop rules about the theft of intellectual property, and about not interfering with a nation’s efforts to bring attacked systems back online. Attacking another nation’s power grid in peacetime is considered out of bounds (Sanger 2016).

2. New Map. The ‘map’ of costs and benefits of Cyberspace has been completely redrawn, for ‘the good guys’ and ‘the bad guys’. The good guys have been shown how costly are insufficient, out-of-date, unprotected internet systems. A few years ago the perceived threats and the costs of their being realized were little discussed, and little prepared for. It is no longer a matter of affordable fixes and embarrassment control,² but one of survival of the business, operationally

²In 2008, in a private discussion late one evening at the US Army War College in Carlisle, Penn with members of its Strategic Studies Institute, the author was asked if he had heard of the ‘theft from the US Treasury’. He had not, and said so, upon which he was told, confidentially, that ‘someone’ had ‘looted the US’ of more than 1 trillion ‘in the seconds it took for the defences to kick in’. The event was never reported in US media (or anywhere else for that matter, to the author’s knowledge).

and or financially. Therefore, cybersecurity companies are very busy. And the bad guys who are having a field day. Global cybercrime costs are estimated as 400 billion in 2014, with a forecast of 2.1 trillion in 2019 (Morgan 2016). There is little doubt which side is ‘winning’.

3. New Players. The number, scale, variety of goods and services on offer, and market for Cyber goods and services are all rising (Cybersecurity Ventures 2016). Construction, energy, mining, and transportation companies are enjoying good days supporting the building of Cyberspace infrastructure. Names such as Tara Global, CrowdStrike, and Kaspersky Lab may not yet be ‘family names’ but everybody working in or who depends on their Cyberspace systems being up and running knows who they are. This includes the bad guys who are working hard to stay ahead of them, a mission made easier because they have none of the implied and explicit constraints of those who, to some degree, value democracy and the rule of law.

5.5 *Consequences for the Future*

It is impossible to state with confidence what the consequences of the Cyberspace are for the future. But, it is reasonable to suggest that consequences already seen and experienced and those that anyone with some imagination can see if they try signal more consequences that will be ever more complicated, connected, costly and valuable.

One is sure to be future installments from the Snowden files, Anonymous and Wikileaks, to mention only the three of the most famous sources.

Assange said WikiLeaks plans to start publishing new material starting this week, but wouldn’t specify the timing and subject. Speaking by video link to an anniversary news conference in Berlin, he said the leaks include “significant material” on war, arms, oil, internet giant Google, the U.S. election and mass surveillance. WikiLeaks hopes “to be publishing every week for the next 10 weeks” (Assange 2016).

Deduction: With every additional installment of masses of information from Cyberspace, the map of its consequences will need to be redrawn if it is to be of continuing use. The drawing of that map will intensify the competition among both those drawing its basic outline and those preparing the legend that will determine what the map shows ... until the next change.

A second consequence is a requirement to think thoroughly about the future context, and not only of what is preferred or expected, but what is not, and what might be very bad. To start and to frame the process early on, the following questions should be asked, listed in no particular order:

1. Whither democracy?
2. Whither diplomacy, and the need to go abroad to ‘lie for your country’?³
3. Whither statehood, and the role of government?
4. Whither Climate Change, and the response?

6 Conclusion

The Cyberspace has had, in two quick decades, enormous consequences for the planet and its inhabitants. There is no sign—none—that the power of Cyberspace’s character and activities to provoke change; good and bad, will soon fade. Therefore, Cyberspace consequences for the planet and its inhabitants will increase in number, in their now familiar self-organizing fashion, for the foreseeable future and probably beyond.

The future will come, whatever mankind does. There are no experts on it. Therefore, a rational, and notably inexpensive way to build competence for whatever an acceptable future will demand is engagement in strategic foresight.⁴

References

- Aeon (2016) The internet as an engine of liberation is an innocent fraud. Retrieved from <https://aeon.co/essays/the-internet-as-an-engine-of-liberation-is-an-innocent-fraud>
- Assange J (2016) WikiLeaks’ Assange promises leaks on US election. Canadian Press, 4 Oct 2016. Retrieved from <http://www.msn.com/en-ca/news/world/wikileaks-assange-promises-leaks-on-us-election-google/ar-BBwYBiG>
- BBC (2016) Swiss endorse new surveillance powers. BBC 25 Sept 2016. Retrieved from: <http://www.bbc.com/news/world-europe-37465853>
- Bell S (2016) Canada’s counter-radicalization efforts have ‘little national coherence,’ Public safety minister says. National Post, 14 Aug 2016. Retrieved from <http://news.nationalpost.com/news/canadas-counter-radicalization-efforts-have-little-national-coherence-public-safety-minister-says>
- Buzan B (1987) An introduction to strategic studies: military technology and international relations. Palgrave Macmillan, London

³On 29 Jul 2016, John O. Brennan, the Director of the Central Intelligence Agency, made clear that while spying on each other’s political institutions is fair game, making data public—in true or altered form—to influence an election is a new level of malicious activity, far different from ordinary spy versus spy maneuvers. See <http://www.nytimes.com/2016/07/31/us/politics/us-wrestles-with-how-to-fight-back-against-cyberattacks.html?&moduleDetail=section-news-2&action=click&contentCollection=Politics®ion=Footer&module=MoreInSection&version=WhatsNext&contentID=WhatsNext&pgtype=article>.

⁴Foresight Canada (FC) definition of Strategic Foresight: The integrated capacity to see, think through and do what needs to be done NOW in the light of history-altering implications of the weak signals of change, while there is still time to act pro-actively and creatively and before hidden opportunities are lost and unseen threats have become crises.

- Carr N (2016) Utopia is creepy: and other provocations. WW Norton & Company, New York
- CBC News (2016) 'He knew I was pregnant.' Woman scrambling for housing after apartment scam. CBC News Toronto, 16 Sept 2016. Retrieved from: <http://www.cbc.ca/news/canada/toronto/rental-scam-follow-1.3766908>
- Consumer Reports (2011) Your security. Consumer reports, June 2011
- Cybersecurity Ventures (2016) Meet the hot cybersecurity companies to watch in 2016. Retrieved from <http://cybersecurityventures.com/cybersecurity-500/>
- Economist (2014) Cyber-security: defending the digital frontier. The Economist, Special Report of 12th Jul 2014
- Foreign Affairs (2016) ISIS' Virtual Puppeteers. Foreign Affairs Daily Post, 23 Sept 2016
- Gibson W (1984) Neuromancer. Ace Book, New York
- Harries D (2016) Scanning. Ottawa workshop for the Canadian Association of the Club of Rome: Climate Change Foresight, 8–9 Aug 2016
- Kasulis K (2016) YouTube may be teaching someone to spy on you. Boston globe, 24 Sept 2016. Retrieved from: <http://www.bostonglobe.com/ideas/2016/09/24/youtube-may-teaching-some-one-spy>
- La Pointe C, Levin PL (2016) Automated war. Foreign Affairs Daily Post, 5 Sept 2016. Retrieved from: https://www.foreignaffairs.com/articles/2016-09-05/automated-war?cid=nlc-fatoday-20160907&sp_mid=52244007&sp_rid=amRzaGFycmllc0BiZWxsLm5ldAS2&spMailingID=52244007&spUserID=MjEwNDg3MDc3MTcwS0&spJobID=1001299689&spReportId=MTAwMTI5OTY4OQS2
- MacFarquhar N (2016) A powerful russian weapon: the spread of false stories. NYT, 28 Aug 2016. Retrieved from: <http://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html>
- McGill A (2016) Can Twitter fit inside the Library of congress? The Atlantic, 4 Aug 2016
- Morgan S (2016) Cyber crime costs projected to reach \$2 trillion by 2019. Retrieved from: <http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#7ac44e733bb0>
- Nakashima E (2016) Powerful NSA hacking tools have been revealed online. Washington Post, 16 Aug 2016. Retrieved from: https://www.washingtonpost.com/world/national-security/powerful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-37533479f3f5_story.html
- New York Times (2016a) Snowden leaks Illegal but were 'a public service,' eric holder says, The New York Times, 1 Jun 2016. Retrieved from: <http://www.nytimes.com/2016/06/01/us/holder-says-snowden-performed-a-public-service.html?action=click&contentCollection=U.S.&module=RelatedCoverage®ion=EndOfArticle&pgtype=article>
- New York Times (2016b) Is democratic national committee email hacker a person or a russian front experts aren't? NYT 28 Jul 2016. Retrieved from: <http://www.nytimes.com/2016/07/28/us/politics/is-dnc-email-hacker-a-person-or-a-russian-front-experts-arent>
- New York Times (2016c) US wrestles with how to fight back against cyberattacks. NYT, 31 Jul 2016. Retrieved from: <http://www.nytimes.com/2016/07/31/us/politics/us-wrestles-with-how-to-fight-back-against-cyberattacks.html?&moduleDetail=section-news-2&action=click&contentCollection=Politics®ion=Footer&module=MoreInSection&version=WhatsNext&contentID=WhatsNext&pgtype=article>
- New York Times (2016d) Hack of Democrats' Accounts was wider than believed, officials say, NYT 11 Aug 16. Retrieved from: http://www.nytimes.com/2016/08/11/us/politics/democratic-party-russia-hack-cyberattack.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region®ion=top-news&WT.nav=top-news&_r=0
- Perlroth N (2016) http://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region®ion=top-news&WT.nav=top-news&_r=0
- Ramzy A (2016) Australia stops online collection of census data after cyberattacks. NYT 10 Aug 2016. Retrieved from: <http://www.nytimes.com/2016/08/11/world/australia/census-cyber-attack.html?ref=world>

- Ruiz RR (2016) Russian hackers leak U.S. star athletes' medical information. Retrieved from: <http://www.theglobeandmail.com/sports/wada-claims-russian-cyber-espionage-group-has-hacked-its-systems/article31849291/>
- Sanger DE (2016) U.S. wrestles with how to fight back against cyberattacks, NYT 30 Jul 2016. Retrieved from: <http://www.nytimes.com/2016/07/31/us/politics/us-wrestles-with-how-to-fight-back-against-cyberattacks.html?&moduleDetail=section-news->
- Satter R, Cheslow D (2016) Apple issues iOS patch to thwart powerful spyware. Boston Globe, 25 Aug 2016. Retrieved from: http://www.bostonglobe.com/business/2016/08/25/apple-boosts-iphone-security-after-mideast-spyware-discovery/9vbGynNGtoCrFJIXVD0mOI/story.html?s_campaign=email_BG_TodaysHeadline&s_campaign=
- Snowden E (2014) NYT 11 Aug 2016. Retrieved from: http://www.nytimes.com/2016/08/11/us/politics/democratic-party-russia-hack-cyberattack.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region®ion=top-news&WT.nav=top-news&_r=0
- Tsygankov A (2016) How cyber power fits into Russia's current foreign policy, *russia direct*, 3 Oct 2016. Retrieved from: <http://www.russia-direct.org/profile/andrei-tsygankov>
- Tremonti AM (2016) *The Current*. 22 Aug 2016. Retrieved from: <http://www.cbc.ca/radio/the-current>
- Waterloo Chronicle (2016) Chinese in Canada feel chill of Beijing's reach. Retrieved from: <http://m.waterloochronicle.ca/news-story/6827912-chinese-in-canada-feel-chill-of-beijing-s-reach>
- Weintraub P (2016) The world-wide cage. Retrieved from: <https://aeon.co/essays/the-internet-as-an-engine-of-liberation-is-an-innocent-fraud>

Author Biography

David Harries earned a Ph.D. in nuclear engineering from the University of London. He served in the Canadian military for several decades, was Director of Curriculum Planning and Deputy Commandant at the National Defence College of Canada, and has directed a MA program at the Royal Military College in Kingston. He has lived in 20 countries and paid working visits to another 93 ones. Six years (1996–2002) were spent based in Jakarta and Singapore and working throughout Asia. From 2004 to 2008 he ran one of the three MA programmes at the Royal Military College of Canada (RMC): *Security and Defence Management and Policy*. Educated as a nuclear engineer, he has worked in the public and private sectors as a senior military officer, as a consultant in personal and corporate security, and as a senior advisor and professor in heavy engineering, national development, humanitarian aid, post-conflict/post-disaster response and recovery, executive development and university education. He is currently based in Kingston, Canada from where he does research, curriculum development, teaching and facilitation of strategic foresight focusing on the family of five security domains, comparative civil-military relations, aboriginal entrepreneurship, leadership and leadingship, human security engineering and society resilience. Dr. Harries is most interested in the dynamics of the relationships among significant actors (individuals, organizations, and societies) and how they are governed by their biases, assumptions and interests as influenced by current events and trends. He is presently Chair of Canadian Pugwash Movement (Peace Nobel Prize 1995) and head of its Foresight Committee, a Fellow of the World Academy of Art and Science, a member of the Board of Directors of the Global Initiatives Project and of ProteusCanada, head of the Leadership and Management community of IdeaConnector.net, Associate Executive Director of Foresight Canada and security foresight facilitator at Carleton University in Ottawa. David is interested in all five security domains, civil-military relations, aboriginal entrepreneurship, human security engineering, peacekeeping, and societal resilience.

Cyberspace

Risks and Benefits for Society, Security and
Development

Ramirez, J.M.; Garcia Segura, L.A. (Eds.)

2017, XVI, 281 p. 17 illus., 13 illus. in color., Hardcover

ISBN: 978-3-319-54974-3