

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Cyber-Security: The Threats from Russia and the Middle East

by Ferry de Kerckhove

December 2019

POLICY PERSPECTIVE

CYBER-SECURITY: THE THREATS FROM RUSSIA AND THE MIDDLE EAST

by Ferry de Kerckhove

CGAI Fellow
December 2019

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute
1800, 421 – 7th Avenue S.W., Calgary, AB T2P 4K9
www.cgai.ca

©2019 Canadian Global Affairs Institute
ISBN: 978-1-77397-109-4

The art of war has changed considerably since the end of the Second World War. In the last 15 years, the centre of gravity has slowly shifted from the Atlantic to the Pacific. The West is increasingly being destabilized. Hybrid warfare and cyber-attacks have become increasingly effective alternatives to both hard and soft power. Russia is a major player in this domain; so is Iran. Other players are joining the fray, most of them hostile to the West, such as Iran and Russia's client states. The barriers between civilian and military are fading quickly. All-out war now happens in a space that's invisible to the naked eye. Not only is such warfare threatening us, but it also has consequences we have barely begun to assess. The divide between good and bad is blurring. Marshall McLuhan said the medium is the message. Today, the medium and the message are an undecipherable continuum where evil and lies coexist with truth and goodwill. Technological prowess increases vulnerability, but technology is also at the heart of corresponding systems of security. Thus, we have fully entered a new arms race where deterrence comes from the other side knowing what you don't want him to discover, but what you want him to fear.

Voltaire said: "If you wish to speak to me, let us start by defining the meaning of our words." In this day and age, this mantra is particularly applicable to the definition of contemporary threats as well as of the targets, or even who is in the sights of Russian and Middle Eastern leaders. "Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. In effect, cyberspace can be thought of as the interconnection of human beings through computers and telecommunication, without regard to physical geography."[1] Consequently, "(c)ybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative."[2]

Discussions focus on whether Russia or China is the heavyweight in terms of threat. Some argue that China is more subtle while Russia is more of a rogue. But it is undeniable that China's attempt to change the fundamental paradigm of international relations, while using and hopefully subduing the existing international order's mechanisms to its advantage, represents a holistic approach and is thus more threatening to the world if it even partly succeeds. Indeed, the planet's centre of gravity is moving from the Atlantic to the Pacific and that means the global threat comes from China. If we needed a reminder, in 2014 Chinese hackers stole the personal information of more than 22 million people connected to U.S. security clearance processes.[3] Not bad for five years ago!

[1] "Cyberspace," What is.com . Available at https://whatis.techtarget.com/definition/cyberspace
[2] "What is Cyber Security?" CISCO. Available at https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
[3] Eric Rosenbach and Katherine Mansted, "How to Win the Battle over Data," *Foreign Affairs*, Sept. 17, 2019. Available at https://www.foreignaffairs.com/articles/2019-09-17/how-win-battle-over-data

The Russian Threat

Of course, Russia is no slouch as a threat, but despite being a nuclear superpower, it still remains a niche player and President Vladimir Putin is a tactician far more than a strategic thinker. Whenever he sees a void, he attempts to occupy the terrain, as he did after President Donald Trump's withdrawal of U.S. troops from Syria. But that does not make Putin less nefarious. One could argue that, to a considerable extent, the West has forced him into that position. From 1992 until Putin's accession to power in 2000 – reminiscent of Dean Acheson's "present at the creation" of a "new old" country – it was humiliating for a proud, albeit misdirected country for 70 years, to be dictated to with little consideration. The sight of Boris Nikolayevich Yeltsin melting down into a buffoon was a disgrace. Indeed, despite François Mitterrand's 1995 warning "never to humiliate Russia",[4] the West did exactly that. It took advantage of the diminished Yeltsin, tried to fast-track the transformation of Russia from Soviet socialism into a "wild, wild East" capitalism[5] even before property laws had been clearly defined, and brought NATO closer to Russia's borders by incorporating some of the former Soviet republics into the fold. Putin considers the latter a betrayal of past agreements and an existential threat. Or probably more accurately, he sees it as an impediment to his vision of Russia at the heart of Eurasia, his ill-defined, Soviet-inspired, geostrategic zone of influence with Russia's re-emergence "as the central actor in Eurasia … as a distinct political and security space."[6] This led to the Crimea takeover and further encroachments in Ukraine, as well as eventually, a dominant role in Syria's future. More recently, Putin has been playing chess master between Turkey and Iran.

As Putin stated: "Unfortunately, our Western partners, having divided the USSR's geopolitical legacy, were certain of their own incontestable righteousness having declared themselves the victors of the 'Cold War'."[7] To Putin, ideology matters little; territory does. This explains why, feeling it has been robbed of its history, space and legacy, "Moscow harbours a strong sense of strategic entitlement and will assert its 'rights' energetically."[8] While the West confidently felt that Russia would see the advantage of globalization, which it was prepared to "teach" to the new student, the actual result was an explosion of nationalism in the face of an alien culture.[9] It is noteworthy that Putin considers the fall of the Soviet Union a catastrophe.

Then came Crimea. Again, there are two perspectives on the takeover. On the one hand, there is the outcome of the fall of the Soviet Union and the hasty march toward independence of the former republics, with existing borders defining the new states. On the latter point, the 1994 Budapest Memorandum on Security Assurances (not "guarantees"), although considered an

[4] On the occasion of the 50th anniversary of the end of the Second World War in Moscow in 1995.
[5] As coined for the author in 1993 by a senior advisor of then-president Boris Yeltsin.
[6] "Russia and Eurasia," Report, Stockholm International Peace Institute. Available at https://www.sipri.org/research/conflict-and-peace/russia-and-eurasia
[7] Tom O'Connor, "Russia's Putin Reveals His Biggest Mistake: Trusting the West," *Newsweek*, Oct. 19, 2017. Available at https://www.newsweek.com/russia-putin-reveal-biggiest-mistake-trusting-west-688998
[8] Bobo Lo, "Russia's Crisis: What It Means for Regime Stability and Moscow's Relations with the World," Policy Brief, Centre for European Reform. Available at https://www.cer.eu/sites/default/files/publications/attachments/pdf/2011/policybrief_russia_19feb09-771.pdf I have used this quotation and the following one in a previous article on Russia. I also use some of my previous text.
[9] See Eduard Ponarin, "The Effect of Globalization on Russia," in "Conflict and Reconstruction in Multiethnic Societies: Proceedings of a Russian-American Workshop," National Academies and the Russian Academy of Sciences, 2001. Available at https://www.nap.edu/read/10879/chapter/11

important landmark, had a single purpose: to convince Ukraine to abandon its nuclear weapons in exchange for a commitment by the signatories to provide it with support: "1. The United States of America, the Russian Federation, and the United Kingdom of Great Britain and Northern Ireland, reaffirm their commitment to Ukraine, in accordance with the principles of the CSCE [Commission on Security and Cooperation in Europe] Final Act, *to respect the Independence and Sovereignty and the existing borders of Ukraine*."[10] The memorandum, although formally signed, is not a treaty. Indeed, "Although signatories 'reaffirm their commitment' to Ukraine in many passages, the memorandum requires them to do almost nothing concrete, in the event that Ukraine's sovereignty – territorial or political – is violated. There aren't any hard enforcement mechanisms."[11] Ukraine is the subject of the memorandum, rather than a full participant. Furthermore, according to Volodymyr Vasylenko, Ukraine's former representative at NATO, who took part in drawing up the conceptual principles and specific provisions of the Budapest memorandum, "the form and content of the Memorandum ... show that, unfortunately, the Budapest talks on giving Ukraine security guarantees did not eventually result in a comprehensive international agreement that creates an adequate special international mechanism to protect our national security."[12]

On the other hand, there is Russia's historical origin. Kiev is older than Moscow and it was the awkward "gift" that Nikita Khrushchev made when he gave Crimea to Ukraine in recognition of the role the Ukrainian communist party played in building his career. Putin the nationalist considered it an aberration, particularly given the location of the Russian fleet in Sebastopol. So, he decided in 2014 to retake it illegally in a bloodless action, knowing full well that neither Ukraine nor the international community would ever have authorized an independent referendum. In fact, Russia goes so far as to suggest that the Budapest memorandum does not apply "if conduct contrary to it occurs because of 'domestic, political or socio-economic factors'."[13]

But the real and continuing threat that Russia poses is the ongoing battle by the un-uniformed "green men" whom Moscow dispatched to Ukraine's eastern border. That threat is underscored by the 10,000+ Ukrainian victims, accompanied by the unending intimidation of some of the former Soviet republics, notably those in the Baltics that had embraced the protection of NATO. The Russian trolls operating against NATO troops in these states are clear evidence of Russia's definitive attempts to destabilize the West and scare these former republics. The post-Soviet republics, in the so-called near-abroad, remain the ongoing focus of Moscow which, for example, assuaged Georgia while engulfing Abkhazia and South Ossetia into its direct control. Furthermore, Russia has re-established a strong presence in the "stans" of Central Asia.

Yet, other than as a nuclear power with an associated outsized effect on international affairs, Russia is a relatively weak country, with low fertility rates, an oil-dependent economy,[14] and

[10] Ukraine, "The Budapest Memorandum of 1994." Available at https://larouchepub.com/eiw/public/2014/eirv41n08-20140221/34-35_4108.pdf
[11] Cody M. Poplin and Benjamin Bissell, "Throwback Thursday: The 1994 Budapest Memorandum," *Lawfare*, Nov. 20, 2014. Available at https://www.lawfareblog.com/throwback-thursday-1994-budapest-memorandum
[12] Volodmyr Vasylenko, "On Assurances without Guarantees in a Shelved Document," day.kiv.ua, Dec. 15, 2009. Available at http://day.kyiv.ua/en/article/close/assurances-without-guarantees-shelved-document
[13] Poplin and Bissell.
[14] See Chas Goldman, "The Kremlin's Key to World Dominance: Climate Change," *The National Interest*, Feb. 19, 2009. Available at https://nationalinterest.org/feature/kremlins-key-world-dominance-climate-change-43942?page=0%2C1

limited industrialization for its level of education and military technology. One of the reasons for the latter is the inability of a still secretive country to ensure that militarily developed technologies benefit the private industrial sector. The U.S. is exactly the opposite, which evoked earlier condemnations of the military-industrial complex by the likes of Canadian-born John Kenneth Galbraith, but this is at the heart of its economic prowess. The mutual denunciation by the U.S. and Russia of the Intermediate-Range Nuclear Forces (INF) Treaty has added to the security uncertainty because Russia has accelerated the development – with recent casualties – of a hypersonic cruise missile, and Trump has declared the U.S. to be well advanced in its own development. It seems that the nature and purpose of U.S. research in the field is different but effective.[15]

Despite Trump's denials, the Mueller report and Clint Watts' testimony on Russia's interference with U.S. elections[16] have amply demonstrated the Russian capacity to wage an all-out disinformation war against the West in order, as a recent Macdonald-Laurier Institute conference illustrated, to break "the political, economic, and military framework of European and North Atlantic cooperation".[17] This was the first attack on the U.S. against which it did not defend itself.

The Macdonald-Laurier Institute sets out Russian behaviour in clear terms: "Russia uses hybrid or asymmetric tactics to advance its goals in Eastern Europe and beyond. Hybrid warfare combines the use of conventional warfare, covert or irregular warfare, cyber attacks, political disinformation, propaganda campaigns, psychological operations and other tactics. It is meant to keep adversaries off balance through information disruption which generates confusion."

An important element is the use of disinformation and offensive cyber-activities. Russian websites have already tried to spread vicious rumours about NATO troops in the Baltics. Closer to home, they have spread rumours about the family history of Canada's former Foreign Affairs minister, Chrystia Freeland, and have worked to manipulate aspects of Baltic history in an effort to marginalize their security concerns.

Russia has a wide range of cyber-tools and resources, including the ability to carry out denial-of-service attacks, develop sophisticated malware and exploit previously unknown software vulnerabilities. Kremlin cyber-warriors are capable of targeting everything from individual mobile phones to the IT infrastructures of entire governments. The Baltic countries have been exposed to these types of threats for some time and are familiar with the danger.[18] A very eloquent description of Russian capabilities can be found in a testimony given by Jakub Kalensky, senior fellow at the Atlantic Council.[19]

[15] Nyshka Chandran, "Here's Where Major Military Powers Stand in the Global Hypersonic Arms Race," CNBC, May 11, 2018. Available at https://www.cnbc.com/2018/05/11/hypersonic-arms-race-us-may-not-be-losing-to-russia-china.html
[16] Clint Watts, "Clint Watts' Testimony: Russia's Info War on the U.S. Started in 2014," *The Daily Beast*, April 10, 2017. Available at http://www.thedailybeast.com/clint-watts-testimony-russias-info-war-on-the-us-started-in-2014
[17] "Russia-Proofing Your Election: Defending Against Disinformation and Cyber-Threats," Macdonald-Laurier Institute Conference, June 11, 2019.
[18] "Russia's Challenge to European and North American Security," Macdonald-Laurier Institute, Sept. 27, 2018. Available at https://www.macdonaldlaurier.ca/photos-videos-russias-challenge-north-american-european-security/
[19] https://disinfoportal.org/testimony-jakub-kalensky/

On Nov. 3, during his Global Public Square program on CNN, Fareed Zakaria cited a Facebook investigation which showed a massive Russian operation aimed at 250,000 followers on 50 Instagram profiles, with a doubling down on its cyber-capability. According to the U.S.'s National Security Agency and to U.K. intelligence, Russia has even managed to piggyback on an Iranian cyber-operation to reach 35 countries to deliver messages purporting to be from Iran. We are talking here of an all-out information war – Trump's denials notwithstanding – against the West, its democracies, its institutions and its values, with the hope of wreaking havoc in co-operative frameworks such as NATO and the EU. France experienced cyber-attacks during its last presidential and parliamentary elections. So did Germany. Canada seems not to be immune, either. The U.K. is in the midst of a crisis regarding a secret report on Russian infiltration. Unfortunately, Trump's unending attacks on U.S. allies within NATO and the EU, and his attacks against the institutions themselves, are dangerously facilitating Russia's destabilizing activities. It is all the more disheartening that, apparently, the president's border wall project is actually shifting funds away from construction projects in Europe designed to help these allies prevent a possible Russian attack.

Yet, the December 2017 U.S. National Security Strategy – a document Trump signed – states very clearly: "Russia uses information operations as part of its offensive cyber efforts to influence public opinion across the globe. Its influence campaigns blend covert intelligence operations and false online personas with state-funded media, third-party intermediaries, and paid social media users or 'trolls'."[20] It goes further: "U.S. efforts to counter the exploitation of information by rivals have been tepid and fragmented. U.S. efforts have lacked a sustained focus and have been hampered by the lack of properly trained professionals."[21] The strategy underscores that Russia and China are "determined to make economies less free and less fair, to grow their militaries, and to control information and data to repress their societies and expand their influence". The size of the threat from a defence perspective is equally clear: "Virtually all modern weapon systems depend upon data derived from scientific and technical intelligence."[22]

This is not to say that the U.S. and other Western nations can't counter the threat or engage in similar activities. In an extraordinary report, "How the U.S. Hacked ISIS",[23] one can discover how Operation Glowing Symphony succeeded in building "a team and an operation that would deny, degrade and disrupt ISIS's media operation". Ironically, the U.S.'s failed 1979 attempt to rescue the hostages at the U.S. embassy in Iran led to a major buildup of special operations forces. The U.S.'s intelligence capabilities nowadays reflect the view of those engaged in counter-cyber-warfare that "it is critical the military is poised to identify what the future holds when we face peer

[20] National Security Strategy of the United States of America. Available at https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf , 35
[21] Ibid.
[22] Ibid., 32
[23] Dina Temple-Raston, "How the U.S. Hacked ISIS," National Public Radio, Sept. 26, 2019. Available at https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis

and near peer adversaries with comparable technologies outside the boundaries of conventional warfare … The enemy will not fight us conventionally, they've told us as much."[24][25]

The Middle East

One must look at the Middle East as a quagmire where every country plays a conflicting role, which adds an incentive to bring cyber-capability into the fields of war. The field is also infested with individuals or groups outside of governmental institutions who have interests and power across regimes and polities, and major stakes in outcomes. Iran is the most sophisticated actor, on par with its arch-enemy Israel, the latter still having a huge technological advantage in addition to nuclear weapons. Recent events paint a picture of a much more sophisticated information/disinformation operation on Iran's part, verging on Machiavellianism.[26]

Iran's history is complex. The present era started with the 1979 Khomeini/ populist/Shia/anti-Wahhabi Sunni/revolution-spawning Hezbollah supporting Syria's Alaouite (aligned with Shia) Hafez al Assad, father of Bashar. This led to the bloody Sunni Iraq/Shia Iran 1980-1988 war with U.S. military aid going to Iraq. This in turn reinforced Iran's hatred for the U.S and its support of Saddam Hussein, feelings already well fed by memories of the U.S.-U.K. overthrow of Iran's nationalist PM Mohammad Mossadegh in the 1950s. Today, Khomeini's successor, Ayatollah Ali Khamenei, has that hatred in his DNA. So do his key partners such as Mohsen Rezaei Mirghaed from the Iranian Revolutionary Guard Corps, former foreign minister Ali Akbar Velayati, secretary of the Supreme National Security Council of Iran Ali Shamkhani, and a few others. Thus, to the extent that the Iran nuclear deal, the JCPOA – Joint Common Program of Action – had not been enshrined in legislation by the U.S., Trump's decision to disown it did not come as much of a surprise to the Iranians, although for economic reasons, they wanted it to stick – and they still want it to survive.

Indeed, while its leaders are motivated by strong feelings against the U.S., Iran is remarkably rational from a policy perspective and is guided by its ability or lack thereof to maintain deterrence against its foes. The JCPOA represented a palatable range of concessions by the regime in exchange for the end of sanctions, the end of foreign military threats and a broad interest on the part of the international community to accept Iran's reintegration in the global commons. Today, the U.S. has no interest, as the key player, in resuming negotiations, ending threats of military action and providing sanctions relief, while the Europeans appear incapable of finding a modality

[24] Diana Stancy Correll, "40 Years Later: How the Iran Hostage Crisis Shaped the Future of Special Operations," Nov. 4, 2019. Available at https://www.militarytimes.com/flashpoints/2019/11/04/40-years-later-how-the-iran-hostage-crisis-shaped-the-future-of-special-operations/

[25] For a more detailed account of Russia's capabilities and objectives, see CSIS' workshop report on Russia's world view: "Russian World-Views: Domestic Power Play and Foreign Behaviour," Canadian Security Intelligence Service, June 2017. Available at https://www.canada.ca/content/dam/csis-scrs/documents/publications/Russian_world_views-en.pdf ; and M. Snegovaya, Institute for the Study of War, "Putin's Information War in Ukraine: Soviet Origins of Russia's Hybrid Warfare," NSI, September 2015. Available at https://nsiteam.com/putins-information-warfare-in-ukraine

[26] I am very grateful to Pierre Razoux from IRSEM in France for developing many of the following ideas at a conference in Montpellier in October, several of which meshed with my own thinking. See my piece on the JCPOA in Antoine Coppolani and Pierre Razoux, "Les Etats-Unis au Moyen-Orient: Evolutions et Perspectives Stratégiques," Institut de Recherches Stratégiques de l'Ecole Militaire (IRSEM), no. 46, 2016. Available at https://www.irsem.fr/data/files/irsem/documents/document/file/928/Etude_Irsem_n46.pdf

to resume trade with Iran outside of the dollar-dominated international market. Trump looks at the 1979-1980 hostage crisis and does not want to suffer a defeat à la Jimmy Carter, which brought Ronald Reagan into the White House. Therefore, Trump is not interested in any reconfiguration until after the U.S. 2020 election. If he is re-elected, all options return to the table. Underpinning all this is the nuclear "holy grail".

While the country is an Islamic state and religion underpins the regime's solidity, Iran is increasingly guided by its national interest, which can be summarized by a) independence as much from the U.S. as from Russia or China, so it always has options without being tied down one way or another; b) regime preservation; c) managing the transition to a post Khomeini/Khamenei generation; which means d) an emphasis on the economy, however difficult and painful under the present circumstances, while e) avoiding being dragged into an open war. Thus, in the recent spat around the Strait of Hormuz, Iran, in conducting or shepherding the attack on the Saudi ships, signalled its ability to wreak havoc in the region while ensuring a minimum loss of lives. As to its relationship with Israel, Iran profoundly despises Prime Minister Benjamin Netanyahu. By underscoring the weakness of the Arab monarchies, Iran is telling Netanyahu's successor that it might be more useful to develop relations with Iran – as the shah did– than to cavort with the Arabs. It should be appreciated that Iran's support of the Palestinian cause has much more to do with embarrassing the Arab nations for not putting pressure on Israel than with any Iranian love for the Palestinians. That support provides them comfort with stooges in the region like Hamas and Hezbollah. Were Israel to actually provide a working state for Palestine, Iran would find an alternative plank to discredit the Arab states.

To operationalize this complex set of relationships, Iran often resorts to cyber-attacks and related stealth instruments. Security agencies estimate that Iran is the main producer of disinformation messages and trolls through local accounts, mainly focusing on Israel, settlements in Palestine, and fake, racially tainted stories. It has become a major power in this regard as well as a prime target of counter-offensives. Indeed, as the *New York Times* reported, the U.S. and Israel jointly developed the now-famous Stuxnet worm: "From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons."[27]

Foreign Affairs[28] recently published a report on the threat Iran represents as a range of experts perceive it. Responses varied. Some were very ideologically driven, even for scholars. A number of the views underscore that, for the U.S., Iran could not be a major threat but that it has a variety of tools to harm U.S. interests, including through asymmetrical warfare. Others were more concerned about the U.S. mismanaging interests and partners in the region. Most recognized that Iran would avoid any form of large-scale warfare. All underlined Iran's ability to mobilize "a range of coercive activities: supporting terrorist groups and proxies, utilizing cyber tools, engaging in

[27] David E. Sanger, "Obama Order Sped up Wave of Cyber Attacks Against Iran," *New York Times*, June 1, 2012. Available at https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
[28] "Does Iran Pose the Ultimate Threat? *Foreign Affairs* Asks the Experts," *Foreign Affairs*, Aug. 13, 2019. Available at https://www.foreignaffairs.com/ask-the-experts/2019-08-13/does-iran-pose-ultimate-threat

hostile maritime activities, developing ballistic missile capabilities, and exploiting psychological and information operations," as Melissa Dalton of CSIS wrote. Dina Esfandiary reminded readers that "Iran has shown that it can work with the US in arenas like Iraq and Afghanistan when their interests align." Jeffrey Feltman pointed to Iranian proxies in Lebanon and Yemen affecting U.S. interests and allies in the region, but few writers commented on the excessive damage that the U.S.'s premier ally, Saudi Arabia, did in Yemen.

Feltman also referred to "the potential for U.S. allies in the region to harm our interests, through reckless foreign policy adventurism and discriminatory internal policies." Mara Karlin expressed serious concerns about the danger of "weak and irresponsible governance across the region" posing a larger threat to the U.S. Elizabeth Rosenberg aptly said that "a demonization of Iran in U.S. foreign policy should not obscure a U.S. focus on other concerns in the region." There was a strong undercurrent of criticism of the U.S. administration's unilateralist approach to Iran. The RAND Corporation's Ariane Tabatabai expressed this in clear terms: "An array of issues challenge and threaten U.S. interests in the region, including fragile and failed states, the lack of resources and opportunities fueling migration, the refugee influx, the terrorism problem, climate change, and growing near-peer interest and influence in the region. Iran exacerbates these challenges in some areas but our myopic focus on Iran doesn't do much to advance our long-term interests in the region."

It is interesting to note that most commentators referred to a range of Iranian capabilities, but cyber wasn't at the top of the list. Support for groups like Hamas or Hezbollah and the growing presence of Iran in Iraq seem to be seen as more ominous. An interesting twist to the recent spat around the Strait of Hormuz is the U.S.'s September cyber-strikes on "Tehran's ability to spread 'propaganda'"... in that such "cyber strikes are seen as a less-provocative option below the threshold of war."[29] Isn't it nice to know that cyber-attacks are a firewall for worse?

The threat to Canada from Iran is somewhat insignificant given the infinitesimal level of relations between the two countries ever since the Harper government adopted the 2012 *Justice for Victims of Terrorism Act*, which allows victims of terrorism to sue countries that are listed as supporters of terrorism. But there is no question that Iran does not harbour good feelings toward us. For years, we have promoted the harshest possible resolutions at the UN condemning Iran's human rights abuses. There is little doubt that Iran would use any opportunity to infiltrate Canada. The only positive aspect from Iran's perspective is that we are sticking with the JCPOA.

The Implications

While it is important to assess the respective threats of foes such as Russia, Iran or China, it is equally critical to understand where the art of war is going in this day and age of major advances in artificial intelligence and quantum physics. An ominous fact, according to experts, is that:

[29] Idrees Ali and Phil Stewart, "Exclusive: U.S. Carried Out Secret Cyber Strike on Iran in Wake of Saudi Oil Attack: Officials," Reuters, Oct. 15, 2019. Available at https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-idUSKBN1WV0EK

"Conventional wisdom has long held that advances in information technology would inevitably advantage 'finders' at the expense of 'hiders.' But that view seems to have been based more on wishful thinking than technical assessment. The immense potential of AI for those who want to thwart would-be 'finders' could offset if not exceed its utility for enabling them. Finders, in turn, will have to contend with both understanding reality and recognizing what is fake, in a world where faking is much easier."[30] In other words, "Stealth technology is living on borrowed time … once quantum sensors are fielded, there will be nowhere to hide."[31]

There is indeed a dark side to this new arsenal in that cyber-attacks by the "good guys" are normalized. It took a long time for the Obama administration to admit to it. But in its military authorization bill last year, Congress allowed the Defense secretary to authorize some cyber-attacks without referring to the White House. Voices in the U.S. are questioning the legality of such attacks.[32] Ron Deibert, director of the Citizen Lab at the University of Toronto's Munk School of Global Affairs, has expressed serious concerns about Saudi Arabia's use of cyber-tools in the murder of journalist Jamal Khashoggi.[33] Escalation is unavoidable in this expanding new domain of war. Given its fundamental stealth nature, control measures such as those enshrined in the consensus report of the United Nations Group of Government Experts (UNGGE) on "Developments in the Field of Information and Telecommunications in the Context of International Security", adopted in July 2015, may look promising in UN legal parlance but are unlikely to make much difference on the invisible ground of cyber-space.[34]

There is little deterrence in cyber to the extent that parties cannot wait to be attacked to prepare for a counterattack. Four-star Gen. Paul Nakasone, director of U.S. Cyber Command, put it squarely: "As we think about cyberspace, we should agree on a few foundational concepts. First, our nation is in constant contact with its adversaries; we're not waiting for adversaries to come to us. Our adversaries understand this, and they are always working to improve that contact. Second, our security is challenged in cyberspace. We have to actively defend; we have to conduct reconnaissance; we have to understand where our adversary is and his capabilities; and we have to understand their intent. Third, superiority in cyberspace is temporary; we may achieve it for a period of time, but it's ephemeral. That's why we must operate continuously to seize and maintain the initiative in the face of persistent threats. Why do the threats persist in cyberspace? They persist because the barriers to entry are low and the capabilities are rapidly available and can be easily repurposed. Fourth, in this domain, the advantage favors those who have initiative."[35]

---

[30] Edward Geist and Marjory Blumenthal, "Military Deception: AI's Killer App," War on the Rocks, Oct. 23, 2019. Available at https://warontherocks.com/2019/10/military-deception-ais-killer-app/
[31] Christian Brose, "The New Revolution in Military Affairs," *Foreign Affairs*, May/June 2019. Available at https://www.foreignaffairs.com/articles/2019-04-16/new-revolution-military-affairs
[32] Edwin Jabatey, "Reassessing U.S. Cyber Operations Against Iran and the Use of Force," *Just Security*, Oct. 17, 2019. Available at https://www.justsecurity.org/66628/reassessing-u-s-cyber-operations-against-iran-and-the-use-of-force/
[33] Temple-Raston.
[34] Note by the Secretary General, "Group of Governmental Experts on the Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations General Assembly, July 22, 2015. Available at https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174; see as well Kristen Eichensehr, "'International Cyber Stability' and the UN Group of Governmental Experts," *Just Security*, July 14, 2015. Available at https://www.justsecurity.org/24614/international-cyber-stability-un-group-governmental-experts/
[35] "An Interview with Paul M. Nakasone," JFQ. Available at https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-Interview.pdf

But there is one fundamental conclusion: Countries like Canada and the United States are the countries "most highly dependent on (today's) technologies," Deibert said, "and arguably the most vulnerable to these sorts of attacks."

Isn't there a saying about the best defence being a good offence? We need to give this some serious thought.

About the Author

Ferry de Kerckhove *was born in Belgium in 1947. He has a B.Soc. Sc. Honours in Economics, an M.A. in Political Science from the University of Ottawa and pursued Ph.D. Studies at Laval University in Québec City.*

He joined the Canadian Foreign Service in September 1973. From 1981 to 1985, he was Economic Counsellor at the Canadian Delegation to NATO. In September 1992, he was posted to Moscow as Minister and Deputy Head of Mission. In 1995 he became Associate Chief Air Negotiator, then Deputy Head of the Policy Branch and Director-General, Federal-Provincial Relations in Foreign Affairs and International Trade. He was named High Commissioner to the Islamic Republic of Pakistan in August 1998. In September 2001, he became Ambassador to the Republic of Indonesia. He was also accredited to Timor Leste.

In September 2003 he joined the Faculty of Social Sciences at the University of Ottawa as a Canadian Center for Management Development Diplomat in Residence. In 2004 he became Director General, International Organizations. In July 2006, he added to his responsibilities the function of Personal representative of the Prime Minister for Francophonie. In 2008 he was named ambassador to the Arab Republic of Egypt.

He retired from the Foreign Service on September 23d, 2011. He is a Senior Fellow at the Graduate School of Public and International Affairs, Faculty of Social Sciences, University of Ottawa, a Fellow of the Canadian Global Affairs Institute, and a Member of the Board of the Conference of Defence Associations Institute. He was the author or co-author of four iterations of the Conference of Defence Association Institute's Strategic Outlook for Canada 2013-16. He is a former board member of WIND Mobile Canada. He is President of Ferry de Kerckhove International Consultants Inc.

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.