THE TALLINN PAPERS
A NATO CCD COE Publication on Strategic Cyber Security

KENNETH GEERS

# PANDEMONIUM: NATION STATES, NATIONAL SECURITY, AND THE INTERNET

Vol. 1, No. 1 2014

## Roles and Responsibilities in Cyberspace

The theme of the 2014 Tallinn Papers is 'Roles and Responsibilities in Cyberspace'. Strategic developments in cyber security have often been frustrated by role assignment, whether in a domestic or international setting. The difficulty extends well beyond the formal distribution of roles and responsibilities between organisations and agencies. Ascertaining appropriate roles and responsibilities is also a matter of creating an architecture that is responsive to the peculiar challenges of cyberspace and that best effectuates strategies that have been devised to address them.

The 2014 Tallinn Papers address the issue from a variety of perspectives. Some of the articles tackle broad strategic questions like deliberating on the stance NATO should adopt in cyberspace matters, or exploring the role small states can play in this domain. Others touch upon narrower topics, such as the right to privacy in the growingly intrusive national security context and whether software manufacturers should be compelled to bear their burden of cyber security by making them liable for faulty software. The thread running through all the papers, however, is their future-looking approach, one designed to inspire discussion and undergird strategic development.

## Submissions

The Tallinn Papers is a peer reviewed publication of the NATO Cooperative Cyber Defence Centre of Excellence. Although submissions are primarily commissioned by-invitation, proposals consistent with the annual theme and dealing with issues of strategic importance will be considered on an exceptional basis. Since the Tallinn Papers are meant for a wide audience, such proposals should assume no prior specialised knowledge on the part of the readership. Authors wishing to submit a proposal may contact the Editor-in-Chief at publications@ccdcoe.org.

# Pandemonium: Nation States, National Security, and the Internet

Kenneth Geers[1]

A long time ago, the author of *Ecclesiastes* wrote: "There is nothing new under the sun." What about the internet? The network of networks should help us to have a more peaceful future, but too often it seems that the internet today is merely a reflection of what came before – including crime, espionage, and warfare – and that the international security environment is still closer to Pandemonium[2] than Paradise. To make matters worse, all of our vices have seemingly been teleported into the realm of science fiction. Cyber security threats are both technological and philosophical wonders: a computer program that destroys nuclear centrifuges thousands of miles away, malware that secretly records everything we do, encrypted code that decrypts only on one target device, and so on.

The internet now plays an important role in national security affairs. Consider just a few recent examples from Europe. Cyber spies have targeted the European Union[3] and member states such as France[4] in a drive for competitive advantage in politics and diplomacy. In the business world, Norway's National Security Authority (NSM) has confirmed at least ten separate network penetrations of Norwegian corporations, while noting that the true figure is undoubtedly much higher.[5] In law enforcement, German police discovered that its servers were compromised.[6] In the military domain, French Navy planes were grounded by

1 Senior Global Threat Analyst, FireEye; Ambassador, NATO Cooperative Cyber Defence Centre of Excellence. This Tallinn Paper is adapted from Kenneth Geers, Darien Kindlund, Ned Moran, and Rob Rachwald, 'World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks,' FireEye (2013).

2 Pandæmonium, which now means "wild and noisy disorder", was the capital of Hell in John Milton's epic poem Paradise Lost.

3 "'Serious" cyber attack on EU bodies before summit,' *BBC* (23 March 2011).

4 Robert Charette, "'Spectacular" Cyber Attack Gains Access to France's G20 Files,' *IEEE Spectrum* (8 March 2011).

5 Chloe Albanesius, 'Norway Cyber Attack Targets Country's Oil, Gas Systems,' *PCMag* (18 November 2011).

6 'Hackers infiltrate German police and customs service computers,' *Infosecurity Magazine* (18 July 2011).

malicious code in the form of the Conficker worm.[7] In the United Kingdom, hackers gained access to the Ministry of Defence's classified networks.[8] All of this takes place in an environment where cyber investigation, prosecution, and retaliation are difficult, and sometimes not even desirable.[9]

The purpose of this essay is modest. It spans the globe once, stopping long enough in numerous countries to record some of the most famous examples of international cyber attack and cyber conflict to date, and attempts to place them within a broader geopolitical context. Hopefully, this short composition will accomplish two things: remind the reader that traditional international conflicts have, as a rule, now drifted into cyberspace; and help set the stage for follow-on papers in this research series by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), which will examine the challenge of securing cyberspace from many new angles in the future.

## Russia

Winston Churchill called Russia "a riddle wrapped in a mystery inside an enigma." Today, cyber defence researchers often make a similar claim: Russia has the world's best hackers, so they can operate quietly and without being caught. There is likely some truth in that, but it seems equally true that Russia has been at least tangentially involved in some of the best-known cases of international cyber conflict to date.

Chechnya is an autonomous republic of the Russian Federation, but Moscow has nonetheless engaged in armed conflict with it since the dissolution of the Soviet Union. From the Chechen Wars, the primary lesson for future cyber war planners is that, in the age of the World Wide Web, the propaganda battle for hearts, minds, and wallets will be fought website by website.[10] In 1998, when Russian ally Serbia was under attack by NATO, anonymous pro-Serbian hackers jumped into the fray, flooding NATO networks with denial-of-service (DoS) attacks and at least twenty-five strains of virus-infected email.[11] In 2007, Russia

7 Kim Willsher, 'French fighter planes grounded by computer virus,' *The Telegraph* (7 February 2009).

8 Nick Hopkins, 'Hackers have breached top secret MoD systems, cyber-security chief admits,' *The Guardian* (3 May 2012).

9 John Leyden, 'Relax hackers! NATO has no cyber-attack plans—top brass,' *The Register* (6 June 2012).

10 Kenneth Geers, 'Cyberspace and the Changing Nature of Warfare,' *Hakin9* E-Book, 19(3) No. 6; *SC Magazine* (27 August 08) 1-12.

11 *Ibid*.

was the prime suspect in the most famous international cyber attack to date – the punitive digital assault on Estonia for having moved a Soviet-era statue.[12] In 2008, there was evidence that computer network operations played a supporting role in Russian military advances during its invasion of Georgia,[13] and Russia was the prime suspect in what U.S. Deputy Secretary of Defense William Lynn called the "most significant breach of U.S. military computers ever", a USB-vector attack on Central Command (CENTCOM).[14] In 2009, Russian hackers were blamed in "Climategate", a breach of university research intended to undermine international negotiations on climate change mitigation.[15] In 2010, the FBI arrested and deported suspected Russian intelligence agent Alexey Karetnikov, who had been working as a software tester at Microsoft.[16]

In response to the spectre of future cyber wars, Russia, like the U.S., China, and Israel, is creating cyber warfare-specific military units[17] and, in an effort to improve its digital defences, is buying old-fashioned typewriters.[18]

## China

China's enormous population and rapidly expanding economy have combined to create a voracious appetite for information, which is sometimes most easily acquired through cyber espionage. Much of this espionage appears to have national security implications, which could, over time, alter the balance of power in the Pacific.

As early as 1999, the U.S. Department of Energy believed that Chinese cyber espionage posed an "acute" threat to U.S. nuclear security.[19] In 2001, following

12 Joshua Davis, 'Hackers Take Down the Most Wired Country in Europe,' *WIRED* (21 August 07).

13 U.S. Cyber Consequences Unit, 'Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008' (August 2009).

14 William J. Lynn, 'Defending a New Domain: The Pentagon's Cyberstrategy,' *Foreign Affairs* 89(5) 97-108 (2010).

15 Will Stewart, Martin Delgado, 'Were Russian security services behind the leak of 'Climategate' emails?' *Daily Mail* (6 December 2009) & RT (23 November 2011) 'Global warning: New Climategate leaks,' *RT*.

16 Anastasia Ustinova, 'Microsoft Says 12th Alleged Russian Spy Was Employee,' *Bloomberg* (14 Jul 2010).

17 Vadim Gorshenin, 'Russia to create cyber-warfare units,' *Pravda* (29 August 2013).

18 Geoffrey Ingersoll, 'Russia Turns to Typewriters to Protect against Cyber Espionage,' *Business Insider* (11 July 2013).

19 Jeff Gerth, James Risen, '1998 Report Told of Lab Breaches and China Threat,' *The New York Times* (2 May 1999).

the mid-air collision between a U.S. Navy EP-3 signals intelligence (SIGINT) aircraft and a People's Liberation Army Navy (PLAN) J-8II fighter, and the prolonged detention of the U.S. crew in China, pro-U.S. and pro-China "patriotic" hackers threatened to take the conflict into their own hands.[20] More recently, China apparently stole the plans for the most advanced U.S. fighter jet, the F-35,[21] and hacked Google, Intel, Adobe, RSA, Lockheed Martin, Northrop Grumman,[22] the New York Times, the Wall Street Journal, and the Washington Post.[23] In a turn toward critical infrastructure, U.S. intelligence agencies believe that Chinese hackers targeted two dozen gas pipeline companies, possibly for sabotage,[24] as well as the U.S. Army Corps of Engineers' National Inventory of Dams.[25]

Outside the U.S., the story is little different. Chinese hackers are believed to have compromised the British House of Commons in 2006,[26] the German Chancellery in 2007,[27] Japanese classified documents in 2011,[28] an air-gapped Indian Navy headquarters in 2012,[29] and in 2013 both the South Korean government[30] and the Australian Security Intelligence Organization.[31]

In response, Chinese officials contend that their country is also a victim of cyber

20 Jeremy Wagstaff, 'The Internet Could Be the Site of the Next China-U.S. Standoff,' *The Wall Street Journal* (30 April 2001).

21 Siobhan Gorman, August Cole, Yochi Dreazen, 'Computer Spies Breach Fighter-Jet Project,' *The Wall Street Journal* (21 April 2009).

22 Michael Joseph Gross, 'Enter the Cyber-dragon,' *Vanity Fair* (1 September 2011).

23 Nicole Perlroth, 'Washington Post Joins List of News Media Hacked by the Chinese,' *New York Times* (1 February 2013) and Nicole Perlroth, 'Wall Street Journal Announces That It, Too, Was Hacked by the Chinese,' *The New York Times* (31 January 2013).

24 Mark Clayton, 'Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage,' *The Christian Science Monitor* (27 February 2013).

25 Bill Gertz, 'Dam! Sensitive Army database of U.S. dams compromised; Chinese hackers suspected,' *The Washington Times* (1 May 2013).

26 Peter Warren, 'Smash and grab, the hi-tech way,' *The Guardian* (18 January 2006).

27 'Espionage Report: Merkel's China Visit Marred by Hacking Allegations,' *Spiegel* (27 August 2007).

28 Justin McCurry, 'Japan anxious over defence data as China denies hacking weapons maker,' *The Guardian* (20 September 2011) and The Indian Express, 'China-based servers in Japan cyber attacks,' *The Indian Express* (28 October 2011).

29 Manu Pubby, 'China hackers enter Navy computers, plant bug to extract sensitive data,' *The Indian Express* (01 July 2012).

30 Neal Ungerleider, 'South Korea's Power Structure Hacked, Digital Trail Leads to China.' *Fast Company* (19 October 2010).

31 Associated Press, 'Report: Plans for Australia spy HQ hacked by China,' *USA Today* (28 May 2013).

attacks. In 2006, the China Aerospace Science & Industry Corporation (CASIC) found spyware on its classified network.[32] In 2007, the Chinese Ministry of State Security stated that foreign hackers were stealing Chinese information, "42%" by Taiwan and "25%" by the United States.[33] In 2009, Chinese Prime Minister Wen Jiabao announced that a hacker from Taiwan had stolen his upcoming report to the National People's Congress.[34] In 2013, Edward Snowden, a former system administrator at the National Security Agency (NSA), published documents suggesting that the U.S. conducted cyber espionage against China;[35] and the Chinese computer emergency response team (CERT) stated that it possessed "mountains of data" on cyber attacks by the U.S.[36]

## United States

Ralph Langner, the most experienced researcher of Stuxnet, contends that there is "only one" cyber superpower in the world: the U.S.[37] In fact, if we narrow our definition of cyber attack to the digital destruction of physical infrastructure, Stuxnet may be the only true cyber attack the world has ever seen.

Analysts typically refer to the innovation and elegance of Stuxnet in quasi-religious terms: multiple zero-day exploits, a forced cryptographic "hash collision",[38] and exceptionally sophisticated sabotage under a veneer of legitimate operational data. This malware is so precise that it becomes active only on certain target network configurations, and parts of it have never been fully understood or even decrypted. In contrast to computer worms such as Slammer and Code Red, Stuxnet did not seek to compromise as many computers as possible, but as few as possible. What more could the cyber war skeptics be waiting for?

The most amazing thing about Stuxnet is that its true purpose was to change

32 Center for Strategic and International Studies, 'Significant Cyber Incidents Since 2006,' p. 2, available at: http://csis.org/files/publication/140204_Significant_Cyber_Incidents_Since_2006.pdf.

33 *Ibid.*

34 *Ibid.*, p. 5.

35 Kenneth Rapoza, 'U.S. Hacked China Universities, Mobile Phones, Snowden Tells China Press,' *Forbes* (22 June 2013).

36 Kathrin Hille, 'China claims 'mountains of data' on cyber attacks by US,' *Financial Times* (5 June 2013).

37 Ralph Langner, 'Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon,' TED talk (March 2011), available at http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html.

38 Dan Goodin, 'Crypto breakthrough shows Flame was designed by world-class scientists,' *Ars Technica* (7 June 2012).

the course of world history. It was designed to help prevent an expansion of the world's most exclusive club, the "nuclear club". To some degree, that means that Stuxnet replaced a squadron of aircraft that would have violated foreign airspace and left a smoking crater in the Earth's surface.[39]

Was Stuxnet an American invention? Apart from Langner, The New York Times thinks so,[40] and Richard Clark, who served three U.S. Presidents as a senior counterterrorism official, said that Stuxnet "very much had the feel to it of having been written by or governed by a team of Washington lawyers."[41] With regard to its uniqueness, numerous other advanced cyber attacks such as Duqu, Flame, and Gauss may all have come from the same organization or nation.[42]

If Stuxnet was the world's first glimpse of cyber war, the attack may have been followed by our first glimpse at a cyber counterattack. A group calling itself the "Cutting Sword of Justice", possibly directly or indirectly supported by Iran, used the "Shamoon" virus to attack the Saudi Arabian national oil company Aramco, deleting data (including office documents and email) on three-quarters of its corporate computers – and replacing them with the image of a burning American flag.[43] Another group called Izz ad-Din al-Qassam launched "Operation Ababil", a series of DoS attacks against U.S. financial institutions including the New York Stock Exchange.[44] More recently, the Wall Street Journal reported that Iran had increased its efforts to compromise U.S. critical infrastructure.[45]

## Middle East

Even during the Cold War, there were many fiery wars in the Middle East. Thus it is not surprising that we have seen numerous examples of cyber conflict against the backdrop of the Arab-Israeli and other regional conflicts.

39 David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (2012) pp. 188-225.

40 *Ibid.*

41 Ron Rosenbaum, 'Richard Clarke on Who Was Behind the Stuxnet Attack,' *Smithsonian Magazine* (April 2012).

42 Boldizsár Bencsáth, 'Duqu, Flame, Gauss: Followers of Stuxnet,' BME CrySyS Lab, presentation at RSA Conference Europe 2012, available at: http://www.rsaconference.com/writable/presentations/file_upload/br-208_bencsath.pdf.

43 Nicole Perlroth, 'In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back,' *The New York Times* (23 October 2012).

44 Danielle Walker, 'Hacktivists plan to resume DDoS campaign against U.S. banks,' *SC Magazine* (8 March 2013).

45 Siobhan Gorman, Danny Yadron, 'Iran Hacks Energy Firms, U.S. Says,' *Wall Street Journal* (23 May 2013).

Since at least the year 2000, pro-Israeli hackers have targeted websites of political and military significance in the Middle East, and pro-Palestinian hackers have retaliated, often against the Israeli economic sector.[46] In 2007, Israel reportedly disrupted Syrian air defence networks by cyber attack, with some collateral damage to its own domestic networks, in order to facilitate the Israeli Air Force's destruction of a suspected Syrian nuclear facility.[47] In 2013, Iranian media reported that the Syrian army had carried out an attack against the water supply in the Israeli city of Haifa. Professor Isaac Ben-Israel, a cyber security adviser to Prime Minister Benjamin Netanyahu, denied the report, but nonetheless opined that cyber attacks on critical infrastructure pose a "real and present threat" to Israel.[48] Often, the trouble with computer hacking is that offensive operations do not need to be highly sophisticated to succeed, even against a target as security-conscious as Israel: in 2012, the ineptly written[49] "Mahdi" malware compromised at least 54 targets in Israel.[50]

All modern nations are to some degree dependent on information technology, and are thus vulnerable to cyber counterattack. In 2009, during Israel's military invasion of Gaza, pro-Palestine hackers briefly paralyzed many Israeli government sites with a distributed denial-of-service (DDoS) attack emanating from at least 500,000 computers. The DDoS consisted of four discrete waves, each stronger than the last, peaking at 15 million junk mail deliveries per second. For example, the Israeli "Home Front Command" website, which plays a key role in national defence communications with the public, was down for three hours. Due to technical similarities with the 2008 cyber attack on Georgia during its war with Russia, Israeli officials surmised that the attack was carried out by a criminal organization in the former Soviet Union, and paid for by Hamas or Hezbollah.[51]

Syria is in the midst of a civil war, and there are several examples of international cyber attacks to examine here. The most prominent hacker group is the Syrian Electronic Army (SEA), loyal to Syrian President Bashar al-Assad. SEA has conducted DDoS attacks, phishing expeditions, pro-Assad defacements, and spamming campaigns against governments, online services, and media that

46 *Supra* note 10.

47 Ward Carroll, 'Israel's Cyber Shot at Syria,' *Defense Tech* (26 November 2007).

48 Yanir Yagna, 'Ex-General denies statements regarding Syrian cyber attack,' *Haaretz* (26 May 2013).

49 Tom Simonite, 'Bungling Cyber Spy Stalks Iran,' *MIT Technology Review* (31 August 2012).

50 Kim Zetter, 'Mahdi, the Messiah, Found Infecting Systems in Iran, Israel,' *WIRED* (17 July 2012).

51 Anshell Pfeffer, 'Israel suffered massive cyber attack during Gaza offensive,' *Haaretz* (15 June 2009).

are perceived as hostile to the Syrian government. SEA has hacked Al-Jazeera, Anonymous, Associated Press (AP), the BBC, the Daily Telegraph, the Financial Times, the Guardian, Human Rights Watch, National Public Radio, the New York Times, Twitter, and more.[52] Its most famous exploit was an announcement via AP's Twitter account that the White House was bombed and President Obama injured, after which stock markets briefly lost more than $200 billion.[53]

In July 2013 alone, SEA compromised three widely used online communications websites: Truecaller, the world's largest telephone directory;[54] Tango, a video and text messaging service;[55] and Viber, a free online calling and messaging application.[56] Successful compromises such as these are significant because they could give Syrian intelligence access to the communications of millions of people, including political activists within Syria who might then be targeted for surveillance, intimidation, or arrest.

To compromise its victims, SEA often sends socially engineered spear-phishing emails to lure opposition activists into opening fraudulent, "weaponised" documents. If the recipient falls for the scam, Remote Access Tool (RAT) software is installed on the victim's computer that can give the attacker keystrokes, screenshots, microphone and webcam recordings, stolen documents, and passwords. Of course, SEA likely sends all of this information to a computer address lying within Syrian government-controlled Internet Protocol (IP) space for intelligence collection and review.[57]

## North Korea

Due to ongoing regional and global tensions, everything that North Korea does is of interest to national security thinkers around the world, especially when it

52 See, e.g., Max Fisher, Jared Keller, 'Syria's Digital Counter-Revolutionaries,' *The Atlantic* (31 August 2011).

53 Sarfraz Manzoor, 'Slaves to the algorithm: Are stock market math geniuses, or quants, a force for good?' *Ottawa Citizen* (25 July 2013).

54 Anupika Khare, 'Syrian Electronic Army Hacks Truecaller Database, Gains Access Codes to Social Media Accounts,' *iDigital Times* (19 July 2013).

55 Jacob Kastrenakes, 'Syrian Electronic Army alleges stealing "millions" of phone numbers from chat app Tango,' *The Verge* (22 July 2013); Chloe Albanesius, 'Tango Messaging App Targeted by Syrian Electronic Army,' *PCMag* (23 July 2013).

56 Warwick Ashford, 'Syrian hacktvists hit second mobile app in a week,' *Computer Weekly* (24 July 2013).

57 Hayley Tsukayama, 'Attacks like the one against the New York Times should put consumers on alert,' *The Washington Post* (28 August 2013).

involves asymmetric capabilities such as weapons of mass destruction (WMD) and computer hacking.

North Korea launched its first cyber attack on U.S. and South Korean government websites in 2009. There was little damage done, but the incident gained wide media exposure.[58] By 2013, North Korean hackers had matured. A group called the "DarkSeoul Gang" is believed to be responsible for high-profile operations against South Korea over a period of at least four years, including DDoS attacks and the insertion of malicious code that wiped computer hard drives at banks, media outlets, ISPs, and telecommunications and financial firms, overwriting legitimate data with political messages. Suspected North Korean attacks on U.S. targets include military units based in South Korea, the U.S.-based Committee for Human Rights in North Korea, and the White House. Such incidents often take place on dates of historical significance, including July 4th, the U.S. Independence Day.[59]

North Korean defectors have described a burgeoning cyber warfare department of 3,000 personnel, likely trained in China or Russia. They believe that North Korea has a growing "fascination" with cyber attacks as a cost-effective way to target conventionally superior foes, and that North Korea is growing increasingly comfortable and confident in this new warfare domain, assessing at least two things: that the internet is vulnerable, and that cyber attacks can put psychological pressure on the West. To this end, North Korea has ensured that its own national servers are not connected to the internet, while simultaneously building a dedicated "attack network".[60]

As with China, North Korea asserts that it too is a victim of cyber attacks. In June 2013, when the North suffered a two-day outage of all of its in-country websites, North Korean reporters denounced "concentrated and persistent virus attacks" and proclaimed that the U.S. and South Korea "will have to take the responsibility for the whole consequences." Pyongyang also noted that the attack took place coincident with Key Resolve, a joint U.S.-South Korean military

58 Choe Sang-Hun, John Markoff, 'Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea,' *The New York Times* (8 July 2009).

59 Symantec, 'Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War,' (27 June 2013), available at: http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war.

60 Max Fisher, 'South Korea under cyber attack: Is North Korea secretly awesome at hacking?' *The Washington Post* (20 March 2013).

exercise. The South Korean Joint Chiefs of Staff denied any connection.[61]

## India and Pakistan

As a final example, it is important to remember that wherever there is historical tension in the "real world", there is now parallel tension in cyberspace. Although a heavily fortified border separates India and Pakistan on a traditional map, the quiet, borderless nature of the internet means that both sides are free to engage in computer hacking, even during peacetime.

In 2009, India announced that Pakistani hackers had placed malware on popular Indian music download sites as a clever and indirect way to compromise Indian systems.[62] In 2010, the "Pakistani Cyber Army" defaced and subsequently shut down the website of the Central Bureau of Investigation, India's top police agency.[63] In 2012, over one hundred Indian government websites were compromised.[64] India, for its part, appears responsible for "Operation Hangover", a large-scale cyber espionage campaign in which Pakistani information technology, mining, automotive, legal, engineering, food service, military, and financial networks were targeted.[65]

## A World Map of Malware

A map based on the cyber attacks that the network security company FireEye discovered in 2013 illustrates the global nature of cyber threats. The red circles represent initial command-and-control (C&C) hacker infrastructure – specifically, the compromised computers and computer addresses from which attackers launched operations in 2013.

The location of the C&C infrastructure does not mean that the attackers themselves were based in these countries. Advanced attackers generally route or proxy their traffic through multiple intermediate third-party compromised networks as a means of obfuscation in order to make attribution more difficult for network defenders; hence the use of the qualifying word "initial".

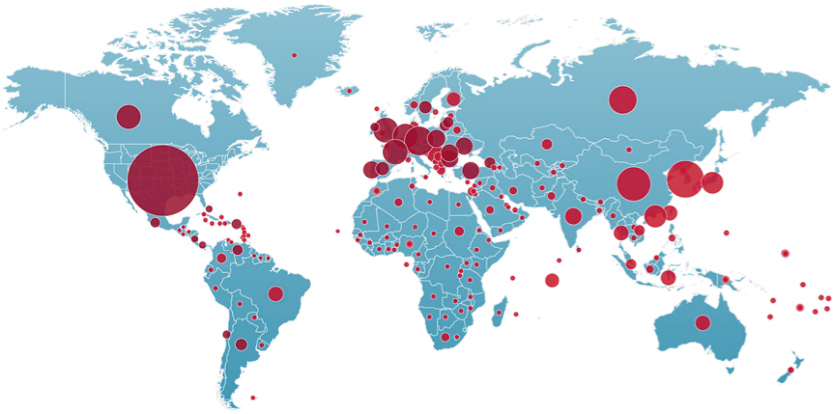
61 Steve Herman, 'North Korea Blames US, South for 'Cyber Attack",' *Voice of America* (15 March 2013).

62 *Supra* note 32, p. 4.

63 'India and Pakistan in cyber war,' *Al-Jazeera* (4 December 2010).

64 Phil Muncaster, 'Hackers hit 112 Indian gov sites in three months,' *The Register* (16 March 2012).

65 Symantec, 'Operation Hangover: Q&A on Attacks,' (20 May 2013), available at: http://www.symantec.com/connect/blogs/operation-hangover-qa-attacks.



According to FireEye data, the top ten countries that were home to malicious C&C infrastructure in 2013 are the United States (24.1%), Germany (5.6%), South Korea (5.6%), China (4.2%), the Netherlands (3.7%), the United Kingdom (3.5%), Russia (3.2%), Canada (2.9%), France (2.7%), and Hong Kong (1.9%). The U.S., probably due to a combination of over 500 million internet-connected computers,[66] a free market philosophy, and plenty of intellectual property to steal, was home to nearly one quarter of the world's initial C&C infrastructure in 2013. The largest international clusters of malicious servers were in Europe and Asia. The primary takeaway from this data is that the world is now swamped in malware –hacker infrastructure was found within the Internet Protocol (IP) space of 206 distinct country code top-level domains in 2013.

The consequence for cyber defenders is that the ubiquitous nature of initial C&C infrastructure allows attackers to change their point of attack to anywhere on the planet. Thus, attackers can and often do "appear" to come from anywhere because there is virtually no place on the Earth today that is malware free, from the Faroe Islands to the Falkland Islands to French Polynesia.

## Conclusion

The internet should help mankind to have a more peaceful future, but for now, international relations in cyberspace still seem closer to Pandemonium than

66 Central Intelligence Agency (CIA) World Factbook, 'United States,' available at: https://www.cia.gov/library/publications/the-world-factbook/geos/us.html.

Paradise. Nations today use computer network operations to defend sovereignty and to project power, and cyber conflicts may soon become the rule rather than the exception. Most cyber attacks do not rise to the level of a national security threat, but in the post-Stuxnet era, the notion of "cyber war" has moved closer to reality.

There is often a strong correlation between the sophistication of a cyber attack and its geopolitical context. In the case of Iran, the question at hand was whether to allow a new nation into the world's nuclear club; it was one of the most important questions that international security decision makers could face. Therefore, it is not surprising that Stuxnet, the malware discovered inside the Iranian nuclear program, was the most advanced malicious code that public researchers have seen.

In the near future, the size of the international cyber stage and the number of actors upon it will grow. Governments will both want and need to flex their digital muscles in order to gain a comparative advantage in political and military affairs as well as to create some level of cyber attack deterrence.

For all nations, an important consideration is the risk of cyber counterattack. The Aramco reprisal, for example, showed that all modern economies are dependent on information technology, and that worldwide connectivity, coupled with the prevalence of cyber vulnerabilities, cuts both ways. Remember that Iraqi insurgents used $26 off-the-shelf software to intercept live video feeds from U.S. Predator drones.[67] There have yet to be any major outages of public critical infrastructure due to cyber attack, but for world leaders, that could be a game changer. One day, we may have a cyber arms control regime or an international non-aggression pact for cyberspace. However, the difficulty of defining malicious code, as well as the challenge of inspecting for it, would make that easier said than done.[68]

Some governments have already begun to take political action to shore up the technical deficiencies in their cyber defences. In 2013, President Obama directed that the U.S. would aid allies who come under foreign cyber attack,[69] and the U.S. and Russia signed an agreement to build a cyber "hotline" similar to that

67 Siobhan Gorman, S., Yochi J. Dreazen, August Cole, 'Insurgents Hack U.S. Drones,' *Wall Street Journal* (17 December 2009).

68 Kenneth Geers, 'Cyber Weapons Convention,' *Computer Law and Security Review* 26(5) 547-551 (2010).

69 Thom Shanker, David E. Sanger, 'U.S. Helps Allies Trying to Battle Iranian Hackers,' *New York Times* (8 June 2013).

used for nuclear scares during the Cold War.[70] Fundamentally, an international problem like cyber security will require an international solution, and the European Union and NATO, as the largest and most cohesive political and military alliances in the world, are the best places to start.

70 Sean Gallagher, 'US, Russia to install 'cyber-hotline' to prevent accidental cyberwar,' *Ars Technica* (18 June 2013).