“Russian Counter-Intelligence and Cyber-Warfare”

by

Patrick R. McElhiney

for

Comp 815 Summer 2017

# of Words: 5,756

Abstract

Information Security is one of the most complex, and important issues facing our nation, as we attempt to learn from the breaches of the past – to secure our future in a hostile world of Russian Counter-Intelligence and Cyber-Warfare. Our democracy is at stake, as we face an adversary that we must cooperate with to prevent nuclear proliferation and terrorism. We must ask ourselves – where do we draw the line regarding what we define as cyber-espionage versus what becomes known as cyber-terrorism. We must fight our cyber battles with bits of information, and secure our systems with new technologies, so we can avoid the temptation to escalate the battle into kinetic space.

# of Words: 5,756

What is Counter-Intelligence?

The definition of “counterintelligence”, is information that is gathered, in addition to activities conducted, to protect (a nation) against espionage, other intelligence activities, sabotage, and/or assassinations which are conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personal, physical, document or communications security programs. Every major, and even minor nations, conduct counterintelligence. This can include the mission of looking at vulnerabilities in one’s own government and closing the discovered holes in security.

There are three types of counterintelligence:

1. Collective counterintelligence, which is gaining information about an opponent’s intelligence collection capabilities that might be aimed at an entity. This could include how the NSA studies telecommunications of Russian intelligence agencies.
2. Defensive counterintelligence, which is thwarting efforts by hostile intelligence services to penetrate the service. This could include the DIA gathering information about Russia’s intelligence operations.
3. Offensive counterintelligence, which is having identified an opponent’s efforts against the system, trying to manipulate these attacks either by “turning” the opponent’s agents into double agents or by feeding them false information they will report home. An example of this would be the CIA or NSA conducting cyber-operations to attack Russia’s intelligence community.

The Federal Bureau of Investigation (FBI) is responsible for counterintelligence operations within the United States. This mission includes keeping track of persons of interest entering and leaving the country to have knowledge of how to intercept and control spies and foreign agents within the United States. The FBI prosecutes hackers, foreign and domestic, which, for an example, deported 10 Russian spies in 2010 from “The Illegals” program.

Counterintelligence is part of intelligence cycle security, which, in turn, is a part of intelligence cycle management. A variety of security disciplines also fall under intelligence security management, and complement counterintelligence, including:

1. **Physical Security** – security measures that are designed to deny unauthorized access to facilities, equipment, and resources, and to protect personnel and property from damage or harm [3].
2. **Personnel Security** – a security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information [4].
3. **Communications Security (COMSEC)** – discipline of preventing unauthorized interceptors from accessing telecommunications in an intelligible form, while still delivering content to the intended recipients. Includes cryptographic security, transmission security, emissions security, and physical security of COMSEC equipment and associated keying material [5].

4. **Information System Security (INFOSEC)** – processes and methodologies involved with keeping information confidential, available, and assuring its integrity. It also refers to:
    - Access controls, which prevent unauthorized personnel from entering or accessing a system.
    - Protecting information, no matter where that information is, i.e. in transit or in a storage area.
    - The detection and remediation of security breaches, as well as documenting those events [6].
5. **Security Classification** – a category to which national security information is assigned to denote the degree of damage that unauthorized disclosure would cause to national defense or foreign relations of the United States and to denote the degree of protection required. There are three such categories:
    a) **Top Secret** – National security information or material that requires the highest degree of protection and the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.
    b) **Secret** – National security information or material that requires a substantial degree of protection and the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security.
    c) **Confidential** – National security information or material that requires protection and the unauthorized disclosure of which could reasonably be expected to cause damage to the national security [7].
6. **Operations Security (OPSEC)** – the process by which we protect unclassified information that can be used against us. OPSEC challenges us to look at ourselves through the eyes of an adversary (individuals, groups, countries, organizations). Essentially, anyone who can harm people, resources, or mission is an adversary [8].

Russian Counter-Intelligence Began Before 2016 U.S. Presidential Elections

It’s important to note that the Russian operations didn’t begin with the 2016 election hacks, and that cyber-espionage has been ever evolving in a post-Cold War world. An example of this evolution is the uncovering of “Ghost Stories”, also known as “The Illegals” program, in which Russian spies have been implanted into legitimate businesses within the United States [9]. The methods and tradecraft of Russian agents have improved over time. The Internet provided the information highway through undersea fiber optic cables. Hackers and spies, alike, have learned how to conceal their identities. Russian agents have developed improved fluency in multiple languages, and through systems-based translations. Counterintelligence agents conduct, detect, and evade surveillance. They use dead drops, brush passes, and information exchange through wireless networks. They also can handle various types of communications equipment, to interfere with surveillance and to report back home undetected, and they also have extensive weapons training [10] [11].

The 2016 Election Hacks Are More Complicated Than Previously Known

The 2016 election hacks were more complex than we initially realized. The attacks spanned 39 out of the 50 states – 37 from their state election systems, and 2 from state-election contractors. The attacks targeted voting machines, voter databases, voting machine software, and campaign finance databases, comprised of 122 local election jurisdictions. For example, in Illinois, Russian hackers tried to delete or alter voting data, and it was detected in July 2016, when unauthorized data was found to be leaving the state election network. They say 90,000 voter records were compromised, just in Illinois alone [12].

The hacking was such a thorn in then President Obama's side, that he had to use a red phone to Russian President Vladimir Putin to insist they stop. This was in addition to the spear phishing campaign that targeted Hillary Clinton's 2016 Presidential campaign and the Democratic National Committee (DNC) [13]. The Russian hackers obtained 19,252 emails with 8,034 attachments from the DNC. The content was then provided to and published by WikiLeaks, which didn't reveal its source. A self-styled hacker going by the moniker Guccifer 2.0 claimed responsibility for the attack, prompting an investigation by the FBI [14]. It should also be noted that the Russian hacking tried to penetrate the Republican National Committee (RNC) as well, but they were unsuccessful.

The politicization of Hillary Clinton's e-mail scandal deserves some corrections to some common misperceptions. The fact is that Hillary Clinton used 13 different devices to access her home-based personal e-mail server, for official State Department business. Hostile foreign actors gained access to the personal email accounts of individuals with whom Hillary Clinton was in regular contact with, and, in doing so, obtained e-mails sent to or received by Clinton on her personal account [15].

It wasn't entirely the Russians that hacked the emails – for instance, Sidney Blumenthal, another State Department employee, had her e-mails hacked and publicly revealed by Romanian hacker Marcel Lehel Lazar. WikiLeaks published e-mails it obtained from other sources – not directly from Hillary Clinton's home-based personal e-mail server. Hillary Clinton's e-mail server was not hacked! Additionally, the U.S. Intelligence Community, made up of 17 different intelligence agencies, in part believes that it was Kremlin-backed Russian hackers that obtained and released the e-mails to WikiLeaks [16] [17].

The Russians also employed a multimillion-dollar army of more than 1,000 Internet trolls. Their purpose was to mold American public opinion with the Kremlin's message – on comment sections of top American websites. On an average work day, a Russian troll posts 50 times on news articles. Each blogger is to maintain 6 Facebook accounts – posting 3 times a day, and discuss in groups two times a day. On Facebook, they were required to obtain 500 subscribers per month, and get at least five posts on each item a day. The Russian trolls also must maintain 10 Twitter accounts, and post fifty times a day on each of them. They were required to get 2,000 new followers per month. The troll army is run by private companies in Russia, such as the Internet Research Agency, located in Saint Petersburg, Russia. The company had over a $10 million-dollar budget in 2014 [19] [20].

Russian Espionage on the Rise Since 2016 Election Hack

Russian espionage is on the rise following the 2016 U.S. Presidential election [2]. They're worried about increased defense spending, in the U.S. and by the North Atlantic Treaty Organization (NATO). They're also worried about the negative perspectives from Congress and the American People, which they refer to as "Russiophobia". They're also trying to gather information to use against the Trump Administration later, just in case, i.e. cyber extortion. They think their activities are helping to prevent war between the U.S. and Russia, while increased spying can lead to greater conflict, i.e. the history of the Cold War.

It is fair to say that the U.S. targets Russia as well. For an example, the National Security Agency intercepts most telecommunications in the world as Signals Intelligence (SIGINT), gathered by its' enormous bank of sensor systems commonly referred to as "Echelon" [21]. Russian President Vladimir Putin self-describes the Internet is a "CIA Project" [22]. It's ultimately this back-and-forth exchange, like a "cat and mouse" game, that creates the differences which are fought in cyberspace. Russian President Vladimir Putin has denied that Russian government hackers targeted the U.S. election system in 2016, even despite there being a consensus in the four organizations that studied the hacks, as part of the U.S. Intelligence Community, that Russia was entirely behind them.

A specific example of how the U.S. has targeted Russia in the past is in 1982, a portion of Russia's Trans-Siberian Pipeline exploded, allegedly due to computer malware implanted in the pirated Canadian software by the Central Intelligence Agency (CIA). It caused the Supervisory Control And Data Acquisition (SCADA) [23] system running the pipeline to malfunction. Flawed turbines were placed inside the gas pipeline. It apparently caused the "most monumental non-nuclear explosion and fire ever seen from space." [24] Other incidents have occurred, but the U.S. doesn't officially take credit for them. One example of obvious plausible deniability was when either the U.S. or Israel deployed malware to take down Iran's uranium enrichment centrifuges with the Stuxnet virus [25], which the International Community realized could have only been developed by the United States.

Vladimir Putin, a spy, now President of Russia

Russian President Vladimir Putin is a former KGB spy from the Cold War era. He served in the KGB starting in 1975, and resigned as rank Lieutenant Colonel on August 20th, 1991. His spy duties overlapped his involvement with politics, early on, in the St. Petersburg Administration from May 1990 through 1996. Then beginning in 1996, he was the Deputy Chief of the Presidential Property Management Department. Then, as of March 26th, 1997, he became the Deputy Chief of Presidential Staff. He was promoted to the First Deputy Chief of Presidential Staff for Regions starting on May 25th, 1998. Next, he served as the Director of the Federal Security Service (FSB), starting on July 25th, 1998. He later served as the 34th Prime Minister from August 16th, 1999 to May 7th, 2000. He became the 2nd President of Russia on May 7th, 2000. He later took the office of the 38th Prime Minister on May 8th, 2008, and once again became the President of Russia (the 4th) starting on May 7th, 2012 [26].

Putin is closely tied to the Russian Intelligence Community, which consists of many different organizations with different purposes – just like the U.S. Intelligence Community. The Foreign Intelligence Service of the Russian Federation (SVR), focuses on foreign intelligence gathering, in addition to military intelligence operations in foreign nations, such as "The Illegals" program, which has been embedding Russian "assets", or intelligence agents, into the United States under the cover of conducting real business within U.S. borders [27]. The Federal Security Service (FSB) of the Russian Federation, was formerly the KGB in the Soviet Union before its collapse in 1991 [28] [29]. This makes Putin a nationalist that is passionate about Russia's military, including foreign intelligence, or counterintelligence operations.

Five Primary Sources for Russian Counter-Intelligence Originating from Within the U.S.

There are five primary sources for Russian Counter-Intelligence that originate from within the United States, at least that I could identify easily:

1. **Defectors** – like Edward Snowden, whom which a U.S. House of Representatives report suggests he may have been a Russian intelligence asset [30] – somewhat weighted on how he has dismissed his relations with the Federal Security Service (FSB), which protects him from the public – including threats towards his life *(off the record)* made anonymously by at least one U.S. official. Snowden is viewed as a hero of Russia, for disclosing state secrets about the United States from his former work as a National Security Agency (NSA) contractor. It is believed that he provided data taken from several hard drives he loaded with Confidential and Top-Secret intelligence from the NSA, including the locations of U.S. assets in other nations, or Special Access Programs (SAP) data, to the Russian Federation. This is primarily the reason for his fleeing from U.S. officials.
2. **California** – which, under a leftist movement, intended to break away from the United States and form a special relationship with Russia [31]. California has a famous pro-Russian Congressman, Rep. Dana Rohrabacher, whom the FBI has warned that Russian intelligence officers were trying to turn him into a Russian asset [32] [33].
3. **Moles** – [34] such as those that have released intelligence about the Trump Administration's ties to Russia, and leaks from U.S. Intelligence agencies – such as EternalBlue [35], which was a National Security Agency (NSA) exploit developed to monitor a targeted computer system, which was stolen by hackers and released by presumably North Korea in the WannaCry ransomware and by Kremlin-backed hackers in the NotPetya ransomware.
4. **Pro-Russian Americans** – 23% of Americans are pro-Russian, with a higher percentage being Republicans [36]. They sympathize with Russia because of the repression they believe the U.S. and its allies cause Russia due to sanctions over the Ukrainian conflict and the Syrian civil war, which Russia supports the Syrian regime headed by Bashar Al Assad.
5. **Trump Administration** – through its infidelity of its transition team and the Trump campaign, in which Trump himself called for Russian hackers to release Hillary's e-mails, and through the private business dealings of the Trump organization with Russian businesses – including potentially a bank close to the Kremlin that was banned by sanctions. The Administration is currently gearing up for a legal battle with Former FBI Director Robert Mohler, whom oversees the Russia probe, and Congress – which is set to

interview Trump, Jr., Paul Manafort, and Jared Kushner about secret meetings with Russian officials during Donald Trump's transition from a private citizen to the world stage of the White House.

Vladimir Putin's Revenge Against Hillary Clinton & Family

It's a well-known fact that Vladimir Putin had a grudge towards Hillary Clinton, because of Hillary's organization of anti-Putin Human Rights campaigning inside Russia, when Putin was running for President the second time [37]. It's believed that Putin then retaliated against Hillary Clinton in the 2016 U.S. Presidential election, with the comprehensive counterintelligence operations and cyber-warfare, including the direction of the release of some of Clinton's e-mails to WikiLeaks [38]. According to Clinton, the emails that her attorney didn't keep records of were between herself and her daughter, Chelsea Clinton, who has a PhD in Foreign Relations. It could merely be a coincidence that Russia's annexation of the Crimean Peninsula of Ukraine occurred after it was 'taken' from Ukraine, with no shots fired, on 2/27/2014 [39] – Chelsea Clinton's [40] 34th birthday. It's probably not also merely a coincidence that Boris Nemtsov, Russia's fallen opposition leader and stark opponent of Vladimir Putin was also assassinated on 2/27/2015 [41], exactly one year later, and on Chelsea Clinton's 35th birthday. Considering how opposed Chelsea Clinton has been to the idea of running for President, despite public support, there is clearly some connection between the missing e-mails and Russia's violations of International Law on the specific dates. I imagine there are a lot of people in the U.S. Intelligence Community that are wondering what was in the emails exchanged between Hillary Clinton and her daughter, Chelsea Clinton, and why they were not preserved as family heirlooms, if the e-mails were indeed merely planning Chelsea Clinton's wedding.

Russia Targets the United States

Vladimir Putin calls the Russian hackers "Patriotic Hackers" – which he blames on Russiophobia, or the fear of the Russian People. He says that the hackers wage war in defense of their homeland, which brought up how in the Russian invasion of Georgia in 2008, hackers inside Russia attacked Georgia's telecommunications systems. Vladimir Putin said, "Hackers are free people, like artists." He criticized the U.S. Intelligence Community's electronic fingerprinting, which pointed to Russia; proclaiming:

> *"Whose fingerprints?"*
> *"All these IP addresses can be faked."*
> *"Do you know how many specialists there are like that?"*
> *"It's not evidence. It's an attempt to put this on us."* [42]
> **-- Vladimir Putin, Russia's 4th President**

Russia's attacks towards the United States have been very targeted – such as hacking into at least 12 nuclear power plants in July 2017, including the Wolf Creek nuclear facility in Kansas. According to a senior Department of Homeland Security official, the Russian hackers are trying to establish backdoors on the plant's systems for later use [43] [44]. It is also widely believed that Russian hackers interrupted C-SPAN's coverage of the House of Representatives by streaming Russian Television in the middle of a floor speech by Rep. Maxine Waters, Democrat – California. The interruption only happened online [45].

The Democratic National Committee's (DNC) emails were hacked in 2016, which painted a rosy picture for Hillary Clinton's win over Bernie Sanders in the 2016 Democratic Primary. The hack was dubbed "Grizzly Steppe" by the Department of Homeland Security [46]. On December 30th, 2016, the Burlington, Vermont Electric Department found code associated with "Grizzly Steppe" on their computers [47]. Also in 2016, the same hackers responsible for hacking the DNC released the medical records of at least four Olympic athletes from the U.S., including those of Simone Biles, Elena Delle Donne, and of the tennis-star sisters, Serena Williams, and Venus Williams [48].

Russia's hackers compromised the State Department's e-mail system in 2015, which allowed them to penetrate through to the White House. Federal Law Enforcement, intelligence, and Congressional officials briefed on the investigation say the hack of the State Department's e-mail system was the "worst ever" cyber-attack intrusion against a Federal agency in the United States. According to CNN – the FBI, the Secret Service, and other U.S. intelligence agencies categorized the attacks as "among the most sophisticated attacks ever launched against U.S. government systems." [49]

In July 2014, Russian hackers targeted oil and gas companies in the United States. The attack was nicknamed "Energetic Bear". Hackers sneaked malware into computers at power plants, energy grid operators, gas pipeline companies, and industrial equipment makers. Some oil and gas companies in Spain and across Europe were also attacked by Russian hackers [50].

In 2014, two Russian Federal Security Service (FSB) officers were indicted for facilitating a massive hack on Yahoo! that compromised roughly 500 million accounts. The hack was targeting Russian journalists, U.S. and Russian Government officials, and private-sector employees at financial, transportation, and other companies [51] [52]. Also in 2014, Russian hackers compromised 76 million household accounts and 7 million small business accounts at JP Morgan Chase [53] [54].

In 2014, Russian hackers stole credit card numbers from retail stores, and accessed Americans' bank accounts. Roman Valerevich Seleznev, a Russian national, was dubbed "one of the world's most prolific traffickers of stolen financial information" by the U.S. Secret Service. He was charged with conspiracy to steal more than $100 Million from companies and banks [55].

In April 2009, Chinese and Russian cyberspies were detected attempting to drop malware into the United States electrical grid's systems [56].

Russia Targets Ukraine

Russia hasn't just hacked the U.S. – but also our allies, including Ukraine. Infrastructure targeted by Russian Hackers in Ukraine include banks, utilities – such as the electric grid, natural gas, and Ukraine's military – specifically its' artillery systems.

On June 17th, 2017, Russia released NotPetya, a variant of WannaCry, which targeted Ukraine's Banking Systems. Ukrainian Cyber Police said that the attack appeared to have been seeded through a software update mechanism built into M.E.Doc, an accounting program that companies working with the Ukrainian government need to use. It could have been avoided if systems were patched with the latest Windows Updates [57].

From 2014 to 2016, Russian APT "Fancy Bear", the same hacker group as the 2016 Presidential Election hack in the U.S., used Android malware to target the Ukrainian Army's Rocket Forces and Artillery. The purpose was to control targeting data for the D-30 Howitzer artillery. The app, used by Ukrainian officers, was loaded with X-Agent spyware, and posted online on military forums. CrowdStrike claims more than 80% of Ukrainian D-30 Howitzers were destroyed [24].

On December 23rd, 2015, there was the Sandworm attack against the Ukrainian power grid. Corporate networks were previously compromised using spear-phishing e-mails with "BlackEnergy" malware. The malware seized SCADA under control, remotely switching substations off. It disabled / destroyed IT infrastructure components, including uninterruptable power supplies (UPS), modems, RTUs, and commutators. It destroyed files stored on servers and workstations with KillDisk malware. It also caused a Denial-of-Service attack on a call-center, to deny customers up-to-date information on the blackout. In total, up to 73MWh of electricity was not supplied [24] [59].

In March 2014, a Russian cyber-weapon called Snake or "Ouroboros" created havoc on Ukrainian government systems. The Snake tool kit began spreading into Ukrainian computer systems in 2010. It performed Computer Network Exploitation (CNE), as well as highly sophisticated Computer Network Attacks (CNA) [24].

Russia's Close Relationship with China

Russia has a close relationship with China, which also hacks into U.S. systems. Chinese spies have taken Intellectual Property from the U.S. Defense Department and U.S. defense contractors, including Lockheed Martin and Boeing. Chinese spies have also been indicted by the FBI for spying and hacking into the U.S.

Naturalized citizen Dongfan Chung, an engineer that was working for Boeing, was the first person convicted under the Economic Espionage Act of 1996. Chung is suspected of having passed on classified information on designs including the Delta IV rocket, F-15 Eagle, B-52 Stratofortress and the CH-46 and CH-47 helicopters. China's espionage and cyber-attacks against the US government and business organizations are a major concern, according to the seventh annual report (issued Sept 2009) to the US Congress of the U.S.-China Economic and Security Review Commission. The report cited that the number of cyber-attacks from China against the US Department of Defense computer systems had grown from 43,880 in 2007 to 54,640 in 2008, a nearly 20 percent increase. Reuters reported that the Commission found that the Chinese government has placed many of its computer network responsibilities under the direction of the People's Liberation Army, and was using the data mostly for military purposes. In November 2005, the United States arrested four people in Los Angeles on suspicion of being involved in a Chinese spy ring. [65]

How Does This Topic Pertain to My Career?

You may be wondering – how does the topic of Russian Counter-Intelligence (CI) and Cyber-Warfare pertain to my career?

(As presented to Michael Jonas' COMP815 – Information Security class on 7/26/2017 at the University of New Hampshire, Manchester)

Regardless of your career path, it's more than likely your organization will be targeted by Russia's cyber warfare and counter-intelligence operations. There are many different types of culprits, and their chosen targets. Some of these are as follows:

- **State-Backed** – cyber espionage targeting major U.S. Government agencies, defense contractors, and all organizations that interact with them.
- **Lone Wolf** – targeting private companies, non-profit organizations, healthcare organizations, defense contractors, and government agencies at all levels.
- **Cyber Terrorist** – targeting major infrastructure, including utilities, healthcare, transportation, and the media.
- **Hacker Group** – targeting virtually anything connected to the Internet.

Kaspersky Labs Software a Threat to National Security of U.S.

Last month, six heads of U.S. Intelligence Community organizations said they don't trust Kaspersky Labs software, in testimony to Congress. Kaspersky is said to be a possible threat to national security. Millions of Americans use Kaspersky. It has been said that the Russian government could use Kaspersky Anti-Virus to spy on U.S. individuals. Kaspersky Labs has denied these claims [59].

Purge of Spies Underway in Russia

A purge of spies is underway in Moscow, which has included treason charges being filed against two high-rank Russian Security Service (FSB) Agents charged with passing confidential information to the Central Intelligence Agency (CIA). Additionally, a cybersecurity expert from Kaspersky Labs is said to have been the target of an investigation pre-dating his employment at Kaspersky Labs, who is also being charged with treason in favor of the United States. There is a report that suggests these men, and another man who is unidentified, were behind the hacking ring targeting the United States – however this may simply be Russia trying to scapegoat individuals for its own handy work [60].

Cyber-Warfare "First Strike" Option

Imagine if there was a Cyber-Warfare "First Strike" option, in which Russia was burrowing its way deeply into the industrial and commercial networks of the U.S. through the deployment of Ransomware across its entire private sector – in which Russia's President could flip a single switch to hold the entire country at ransom. Is this option closer than we think? [61]

President Trump still isn't sure it was Russia

> *"I think it was Russia but I think it was probably other people and/or countries, and I see nothing wrong with that statement. Nobody really knows. Nobody really knows for sure."* [62]
>
> --President Trump (on a visit to Poland, following two meetings with Russian President Vladimir Putin)

Since then, the U.S. and Russia are reportedly in talks to create a cyber security working group, according to Russia's RIA news agency on 7/20/2017. The report cites the special presidential envoy on cyber security in Russia, Andrey Krutskikh. President Trump said he discussed the idea with Russian President Vladimir Putin at the Group of 20 nations in Hamburg, Germany. Senior Republicans on the Hill said Moscow could not be trusted, and President Trump later tweeted that he did not think it could happen [63] [64].

Is Russia's Government liable for the hacking, and just trying to make things look convenient?

Forward Thinking

If you take anything away from this paper, it should be that you cannot trust Russia in recent times, because of their Counter-Intelligence and Cyber-Warfare that they have been conducting against the United States and its allies for years. If you use Kaspersky Anti-Virus, you should remove it, and you should also always keep Windows Updates enabled, so that you are not vulnerable to zero-day exploits like EternalBlue – there will be more viruses and malware in the future, likely originating from Russia, in addition to other regions around the world.

If you ever have any issues with Russia hacking into your systems, you should hire an expert, and be in contact with the Federal Bureau of Investigation (FBI), as they oversee counter-intelligence within the United States. For now, it appears it's going to be up to President Donald Trump and his Cabinet, as well as the U.S. Intelligence Community, as to how we respond to the Russian intelligence operations targeting American interests – unless there is significant evidence uncovered regarding collusion between Trump associates and the Russian government. If it ends up like the healthcare bill, there could become an issue where the President of the United States doesn't have the interests of most of the United States population at heart, in which we would need to find new leadership for vital issues, including how to address Russia's cyber operations when they target American interests.

Closing

One thing is certain – the threats posed to the United States from Russian counterintelligence and cyber-warfare must be taken seriously, and the Information Technology industry needs to change its practices to protect the U.S. from cyber threats, regardless of where they originate from. While the threats are quite simple in nature, dealing with them is an entire topic, or set of topics on its own.

# of Words: 5,756

References:

1. *Counterintelligence*, Wikipedia, https://en.wikipedia.org/wiki/Counterintelligence, Retrieved 7/16/2017
2. *Russia steps up spying efforts after election*, Pamela Brown, Shimon Prokupecz, and Evan Perez on CNN, http://www.cnn.com/2017/07/06/politics/russia-steps-up-spying-efforts-after-election/index.html, 7/6/2017
3. *Physical security*, Wikipedia, https://en.wikipedia.org/wiki/Physical_security, Retrieved 7/21/2017
4. *Personnel security*, IT Law Wiki, http://itlaw.wikia.com/wiki/Personnel_security, Retrieved 7/21/2017
5. *Communications security,* Wikipedia, https://en.wikipedia.org/wiki/Communications_security, Retrieved 7/21/2017
6. *Information Systems Security,* Techopedia, https://www.techopedia.com/definition/24840/information-systems-security-infosec, Retrieved 7/21/2017
7. *Security Classification,* The Free Dictionary, http://www.thefreedictionary.com/Security+classification, Retrieved 7/21/2017
8. *Operations Security (OPSEC),* DODEA, http://www.dodea.edu/Offices/Safety/OPSEC.cfm, Retrieved 7/21/2017
9. *Illegals Program*, Wikipedia - https://en.wikipedia.org/wiki/Illegals_Program, Retrieved 7/8/2017
10. *Russian Spies & Operation Ghost Stories: HUMINT Tradecraft Revealed*, 14Charlie on SOFREP, https://sofrep.com/33494/humint-tradecraft-russian-spies-operation-ghost-stories/, 3/4/2014
11. *HUMINT Snapshot: Working Through Deep Cover Roles*, 14Charlie on SOFREP.COM, https://sofrep.com/31174/humint-snapshot-working-deep-cover-roles/, 1/10/2014
12. *Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known*, Michael Riley and Jordan Robertson on Bloomberg, https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections, 6/13/2017
13. *Hillary Clinton blames high-up Russians for WikiLeaks releases*, Lauren Carroll on Politifact, http://www.politifact.com/truth-o-meter/statements/2016/oct/19/hillary-clinton/hillary-clinton-blames-russia-putin-wikileaks-rele/, 10/19/2016
14. *2016 Democratic National Committee email leak,* Wikipedia, https://en.wikipedia.org/wiki/2016_Democratic_National_Committee_email_leak, Retrieved 7/13/2017
15. *FBI releases Hillary Clinton email investigation documents*, Matt Zapotosky and Rosalind S. Helderman at The Washington Post, https://www.washingtonpost.com/world/national-security/fbi-releases-hillary-clinton-email-investigation-documents/2016/09/02/21bd3682-704c-11e6-8365-b19e428a975e_story.html?utm_term=.a30c8e8b8c8c, 9/2/2016
16. *Trump Misleads on Russian Meddling: Why 17 Intelligence Agencies Don't Need to Agree*, Stephen Crowley on The New York Times, https://www.nytimes.com/2017/07/06/us/politics/trump-russia-intelligence-agencies-cia-fbi-nsa.html, 7/6/2017

# of Words: 5,756

17. *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security,* Director of National Intelligence, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national, 10/7/2016
18. *James Clapper Corrects Left's Narrative on Russia Election Interference: 'Not All 17' Intel Agencies Affirmed*, Aaron Klein on AFP, http://www.breitbart.com/big-government/2017/05/09/deflated-clapper-contradicts-claim-17-u-s-intel-agencies-concluded-russia-interfered-2016-election/, 5/9/2017
19. *1,000 Paid Russian Trolls Spread Fake News on Hillary Clinton, Senate Intelligence Heads Told*, Mary Papenfuss at Huffington Post, http://www.huffingtonpost.com/entry/russian-trolls-fake-news_us_58dde6bae4b08194e3b8d5c4, 3/31/2017
20. *Documents Show How Russia's Troll Army Hit America,* Max Seddon on BuzzFeed, https://www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america?utm_term=.vfedYrzKe#.vg2erX3vj, 6/2/2014
21. *National Security Agency*, Wikipedia, https://en.wikipedia.org/wiki/National_Security_Agency, Retrieved 7/9/2017
22. *Putin calls internet a 'CIA project' renewing fears of web breakup*, Ewen MacAskill at The Guardian, https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia, 4/24/2014
23. *SCADA,* Wikipedia, https://en.wikipedia.org/wiki/SCADA, Retrieved 7/16/2017
24. *Cyberwarfare by Russia*, Wikipedia, https://en.wikipedia.org/wiki/Cyberwarfare_by_Russia, Retrieved 7/8/2017
25. *Stuxnet*, Wikipedia, https://en.wikipedia.org/wiki/Stuxnet, Retrieved 7/16/2017
26. *Vladimir Putin,* Wikipedia, https://en.wikipedia.org/wiki/Vladimir_Putin, Retrieved 7/8/2017
27. *Foreign Intelligence Service (Russia)*, Wikipedia, https://en.wikipedia.org/wiki/Foreign_Intelligence_Service_(Russia), Retrieved 7/8/2017
28. *Federal Security Service,* Wikipedia, https://en.wikipedia.org/wiki/Federal_Security_Service, Retrieved 7/8/2017
29. *KGB,* Wikipedia, https://en.wikipedia.org/wiki/KGB, Retrieved 7/8/2017
30. *House report: Edward Snowden in contact with Russian agents*, Eric Geller at Politico, http://www.politico.com/story/2016/12/edward-snowden-russian-agents-house-report-232917, 12/22/2016
31. *Report: Russia, Putin Back Left-Wing California Secession Movement*, Assemblyman Tim Donnelly on Breitbart, http://www.breitbart.com/california/2016/12/08/secession-calexit-putin-russia-california-secede/, 2016
32. *Dana Rohrabacher,* Wikipedia, https://en.wikipedia.org/wiki/Dana_Rohrabacher, Retrieved 7/21/2017
33. *Putin's favorite congressman*, Isaac Arnsdorf and Benjamin Oreskes at Politico, http://www.politico.com/story/2016/11/putin-congress-rohrabacher-trump-231775, 11/23/2016
34. *Is There a Russian Mole Inside the NSA? The CIA? Both?*, Daily Beast, Kevin Poulsen at The Daily Beast, http://www.thedailybeast.com/is-there-a-russian-mole-inside-the-nsa-the-cia-or-both, 2017
35. *EternalBlue*, Wikipedia, https://en.wikipedia.org/wiki/EternalBlue, Retrieved 7/8/2017

# of Words: 5,756

36. *Anti-Russian sentiment,* Wikipedia, https://en.wikipedia.org/wiki/Anti-Russian_sentiment, Retrieved 7/8/2017
37. *Why Putin hates Hillary,* Michael Crowley and Julia Ioffe, http://www.politico.com/story/2016/07/clinton-putin-226153, 7/25/2016
38. *Putin's Revenge,* Michael Crowley at Politico, http://www.politico.com/magazine/story/2016/12/russia-putin-hack-dnc-clinton-election-2016-cold-war-214532, 12/16/2016
39. *Annexation of Crimea by the Russian Federation*, Wikipedia, https://en.wikipedia.org/wiki/Annexation_of_Crimea_by_the_Russian_Federation, Retrieved 7/21/2017
40. *Chelsea Clinton,* Wikipedia, https://en.wikipedia.org/wiki/Chelsea_Clinton, Retrieved 7/21/2017
41. *5 Convicted in Killing of Boris Nemtsov, Russian Opposition Leader,* Ivan Nechepurenko at The New York Times, https://www.nytimes.com/2017/06/29/world/europe/boris-nemtsov-russia.html, 6/29/2017
42. *Patriot games: The murky world of Russian hacking,* Tim Lister at CNN, http://www.cnn.com/2017/06/02/politics/vladimir-putin-russian-hacking/index.html, 6/2/2017
43. *Hackers breached at least a dozen US nuclear power sites – and officials are zeroing in on a familiar player,* Sonam Sheth at Business Insider, http://www.businessinsider.com/officials-believe-russia-hacked-us-nuclear-power-sites-2017-7, 7/7/2017
44. *Russia suspect in power plant hacks*, Bloomberg on The Journal Gazette, http://www.journalgazette.net/news/us/20170708/russia-suspect-in-power-plant-hacks, 2017
45. *C-SPAN Live Online Broadcast Taken Over by Russian Television,* Alicia Powe at Western Journalism, http://www.westernjournalism.com/c-span-live-online-broadcast-taken-over-by-russian-television/, 7/13/2017
46. *GRIZZLY STEPPE – Russian Malicious Cyber Activity*, United States Computer Emergency Readiness Team (US-CERT), https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity, 12/29/2016
47. *Vermont utility finds alleged Russian malware on computer*, Evan Perez at CNN, http://www.cnn.com/2016/12/30/us/grizzly-steppe-malware-burlington-electric/index.html, 12/31/2016
48. *A Russian Hacking Group Has Released US Olympians' Medical Records,* Sheera Frenkel at BuzzFeed, https://www.buzzfeed.com/sheerafrenkel/simone-biles-serena-williams-among-olympic-athletes-to-have?utm_term=.yyXlOX220#.odvELpJJk, 9/13/2016
49. *How the U.S. thinks Russians hacked the White House,* Evan Perez and Shimon Prokupecz at CNN, http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/index.html, 4/8/2015
50. *Russia attacks U.S. oil and gas companies in massive hack*, Jose Pagliery on CNN, http://money.cnn.com/2014/07/02/technology/security/russian-hackers/index.html, 7/2/2014

# of Words: 5,756

51. *Russian Spies Charged in Massive Yahoo Email Hack*, Ken Dilanian at NBC News, http://www.nbcnews.com/tech/tech-news/russian-spies-charged-massive-yahoo-email-hack-n733716, 3/15/2017
52. *The Yahoo hack is the clearest sign yet that Russia has merged criminal hacking with a larger mission,* Natasha Bertrand at Business Insider, http://www.businessinsider.com/yahoo-hack-russia-hacking-2017-3, 3/18/2017
53. *Report: Russian hackers behind JPMorgan Chase attack*, Chris Woodyard at USA TODAY, https://www.usatoday.com/story/money/business/2014/10/04/jpmorgan-chase-cyberattack-russians/16717499/, 10/7/2014
54. *JPMorgan Chase Hacking Affects 76 Million Households*, Jessica Silver-Greenberg, Matthew Goldstein, and Nicole Perlroth at The New York Times, https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/, 10/2/2014
55. *Russian hacker arrested for widespread U.S. credit card data theft*, CBS News, http://www.cbsnews.com/news/russian-hacker-arrested-for-widespread-u-s-credit-card-data-theft/, 7/7/2014
56. *China and Russia hack into US power grid*, Alex Spillius on The Telegraph, http://www.telegraph.co.uk/news/worldnews/asia/china/5126584/China-and-Russia-hack-into-US-power-grid.html, 4/8/2009
57. *'Petya' Ransomware Outbreak Goes Global*, Brian Krebs on KrebsOnSecurity.com, https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/, 6/27/2017
58. *December 2015 Ukraine power grid cyberattack*, Wikipedia, https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack, 2015
59. *Congress Casts a Suspicious Eye on Russia's Kaspersky Lab*, David Welna on NPR, http://www.npr.org/sections/parallels/2017/07/05/535651597/congress-casts-a-suspicious-eye-on-russias-kaspersky-lab, 7/5/2017
60. *Russian spy purge after suspected leaks to U.S. intelligence*, Jose Pagliery, Matthew Chance, and Emma Burrows on CNN, http://money.cnn.com/2017/02/01/news/fsb-kaspersky-arrests/index.html, 2/1/2017
61. *Hacking Hospitals and Holding Hostages: Cybersecurity In 2016*, Forbes, https://www.forbes.com/sites/kalevleetaru/2016/03/29/hacking-hospitals-and-holding-hostages-cybersecurity-in-2016/#650ad9407d59, 3/29/2016
62. *Trump and Putin find chemistry, draw criticism in first meeting*, Roberta Rampton and Jeff Mason at Reuters, https://www.yahoo.com/news/trump-calls-putin-meeting-honor-cites-very-good-143739467.html, 7/7/2017
63. *Russia, U.S. in talks to create cyber security working group: RIA*, Denis Pinchuk, Vladimir Soldatkin, and Andrew Osborn at Reuters, http://www.msn.com/en-us/news/world/russia-us-in-talks-to-create-cyber-security-working-group-ria/ar-AAoucbH, 7/20/2017
64. *Moscow in talks with U.S. to create cyber working group: RIA report*, Denis Pinchuk, Vladimir Soldatkin, Ayesha Rascoe, Mark Hosenball, Dustin Volz, Andrew Osborn, John Walcott, and Tom Brown at Reuters, https://www.reuters.com/article/us-russia-us-cyber-envoy-idUSKBN1A51MM, 7/20/2017
65. *Chinese intelligence activity abroad,* Wikipedia, https://en.wikipedia.org/wiki/Chinese_intelligence_activity_abroad, Retrieved 7/22/2017

# of Words: 5,756