Nation States: Why They Hack

Motivations That Drive Nation-States To Participate In Various Cyber Activity

China - North Korea - Russia - Iran - Israel - United States
We know that hackers hack for a variety of reasons. Some hack because they are greedy or have criminal motives. Some hack to satisfy their egos or gain peer recognition. Some hack alone, and some hack in groups. But many hackers, or more accurately “hacktivists,” join groups like Anonymous in order to demonstrate their dissatisfaction with powerful organizations—such as corporations and governments who fail to share their world views.

These hackers don’t consider themselves to be bad actors. They see their activity in a positive light, viewing themselves as contributors to a greater body of knowledge, and often hacking without a clear vision of the second-order effects of their actions.

Another category of hacker supports nation-state strategy by operating in the cyber domain. These hackers are difficult to categorize, since they may be directly employed by an arm of a national government (ex., the Chinese PLA). Or they may be from an organized crime entity employed by a national government. Think of recent hacks against JP Morgan Chase, which were attributed to an undefined group in Russia. Understanding the motivation of hackers and the organizations whom they are associated with, is essential to understanding their tactics. Knowing one’s enemy is a fundamental concept in kinetic warfare and is equally important, albeit more difficult, in the cyber environment.

I think it is valuable to explore nation-state, and nation-state-sponsored hackers, because they are generally resourced the best—and their collective motivations run across the spectrum. Because nation-state supported hackers are funded extremely well relative to small groups and individuals, they can be particularly formidable adversaries for other countries and for commercial industry, regardless of vertical. In short, nefarious nation-state-sponsored cyber activity can have devastating effects on a country’s national security and its economy.

All nation-states are not created equal, and like individual hackers, each has a different motivation and level of cyber capability. As we look at the cyber terrain from a global perspective, we see several countries that surface in the media most often: China, North Korea, Russia, Iran, Israel, and the US.

- China -

If you read the daily news you can usually find a story related to China conducting some form cyber exploitation—often against the United States. There are a number of tangible examples of US intellectual property (IP) making its way to China. Defense contractors that support the US Department of Defense have been ideal cyber targets for the Chinese government to exploit. This is mainly due to their knowledge and security clearance to see sensitive material. It’s important to understand that the Chinese don’t limit targets to the US Military or government. Indeed, every sector of the economy is at risk. So it’s worthwhile to understand why the Chinese government seemingly operates on the wire with little regard for the ethical implications of its actions.

There are two overarching reasons why the Chinese have the dubious distinction of being global leaders in cyber espionage. First, the government is trying to establish a regional hegemon in the Eastern Pacific. Second, the Chinese government has been bitten by the capitalism bug, and realizes that to be a true global economic power it needs to be an innovation leader—solely being a mass producer isn’t enough.

Following World War II, the US established itself as one of two global superpowers, and arguably the only superpower in the Pacific region. At the same time China, after resolving its civil war, which had been raging prior to World War II, was firmly established as the second major Communist country in the world, along with USSR. Like USSR, China developed an acute mistrust of Western democracy, and of Western capitalism in particular. In
realidad, the mistrust already existed during the colonial period in the 19th century and the early part of the 20th Century.

Communist philosophy elevated the mistrust to a much more significant level. If we connect the dots, we see China, a Communist government with an innately paranoid view of the rest of the world, squaring off against the symbol of democracy and capitalism in what the Chinese perceive as its own backyard. So over the past 60 years, China has been trying to establish itself as the regional power by trying to catch up to the US, militarily and technologically. The Internet has made it infinitely more convenient for the country to close the technological gap with the US military.

Now let’s talk about innovation…

In spite of the obvious ethical implications of stealing intellectual property, the Chinese government is comfortable with pilfering intellectual property for the greater good of its society and economy. China has the unenviable task of providing healthcare to over 1.4 billion citizens. Facing this challenge, the government is forced to turn to technology in order to reduce the burden on its healthcare system. It is no surprise that China looks to the West for technology solutions, and as the recognized leader in medical technology innovation, the US is a primary target. Between 2013 and 2014, Chinese hackers targeted 18 companies, forcing the healthcare sector to invest an additional $160 million in security for medical and pharmaceutical companies. Interestingly, this apparent surge in healthcare cyber exploitation coincides with Chinese government investment in healthcare and with the subsequent boom in the Chinese healthcare sector.

From a broader perspective, we know that the Chinese government is the driving force behind the country’s impressive economic growth over the past 30 years. Since 1978, following the shift to a market-based economy, albeit still under Communist Party control, China has averaged about 10 percent GDP growth per year. To feed the engine of economic growth, China recognized the need to ramp up its ability to innovate. To meet that demand, China has demonstrated a willingness to close the innovation gap with peer competitors by stealing intellectual property, as demonstrated by the indictment of five Chinese nationals last year for conducting cyber espionage against prominent US companies representing the energy and utility, services, and technology sectors.

- Democratic People’s Republic of Korea -

“The motivation behind Democratic People’s Republic of Korea hacking is rooted in a mix of retribution, paranoia, and the immature behavior of an erratic leader.”

The Democratic People’s Republic of Korea (DPRK) is about as far from a democratic republic as a country can get. It is certainly not a government “of” its citizens. The country has been dominated by a small group that exercises complete control over every aspect of North Korean society. Leading the handful of power brokers has been the “Supreme Leader,” a title which has belonged to three men since Korea was partitioned following World War II.
The first two “Supreme Leaders,” Kim Il-sung and Kim Jong-il, established cults of personality among North Koreans and were viewed as eccentric on the world stage. Throughout their reigns, the DPRK was involved in a number of incidents, most of which involved some form of military action intended to provoke a reaction from the Republic of Korea (ROK), and her most steadfast ally, the United States. There have been over 150 incidents between the DPRK, the ROK, and the US since the Korean Conflict. Some of those conflicts have resulted in the deaths of South Korea citizens, military personnel, and US service members.

The current Supreme Leader, Kim Jong-un, has continued his predecessor’s legacies of maintaining a large and imposing conventional military, and has established a militaristic presence in the cyberdomain. However, Kim Jong-un is somewhat hampered in his efforts to establish the DPRK as a dominant player in the cyberworld, because DPRK cyber capability is rudimentary, particularly compared to the other nations we will discuss. In spite of resource constraints, the DPRK is working hard to establish a credible cyber capability. Like the Chinese Government, the DPRK is believed to be building a cyberarmy, and it is widely known that it has invested heavily in an elite cyber espionage group called Bureau 121.

The motivation behind DPRK hacking is rooted in an interesting mix of paranoia and retribution. The paranoia is similar to the Chinese Government’s view of the United States as a military and economic threat because it perceives the US as meddling in Eastern Pacific affairs. In the case of the DPRK, the paranoia is amplified to the extreme. The deep distrust that the DPRK harbors toward the West and the ROK, its neighbor to the south, is rooted in the Korean Conflict, which ended with an armistice in 1953. The ROK and DPRK are literally still at war, and both countries have maintained a wartime footing since the armistice. As the aggressor, the DPRK doesn’t hesitate to provoke the ROK whenever it serves its purpose. As an example, the DPRK is alleged to have conducted cyber attacks on ROK government and media organizations, coincident with the Korean Conflict Anniversary in 2013.

The recent cyber attack on Sony Pictures is particularly interesting because it appears to go further than what we typically see from the hacktivist community. Generally, hacker groups attempt to make visible statements expressing their displeasure with an organization or government by defacing a website or temporarily disrupting business operations. In the Sony case, the group identified as the Guardians of Peace, and allegedly affiliated with the DPRK, was responding to a discrete event and identified a specific desired short-term outcome, (i.e., Don’t release the movie The Interview). This was a remarkable and unprecedented demand facilitated in cyberspace.

North Korea’s response to the release of the movie was both impulsive and excessive by democratic standards. But the response is not surprising given the previous erratic and adolescent behavior of Kim Jong-un. It is as if the Supreme Leader, by proxy, lashed out like a young child on a playground, “getting back” at a playmate for name-calling. In this case, the “lashing out” is the hack, and “getting back” is Sony’s harsh economic loss. Generally unknown, the Guardians of Peace allegedly drove the behavior of a major motion picture corporation and successfully disrupted the corporation’s business operations. In military parlance, that’s called a soft kill, which can be every bit as effective as a hard kill.
Perhaps most interesting, and at the same time most concerning, is the notion that the Sony hack was an act of terrorism, which reasonable people may conclude. The FBI defines terrorism as “an act that appears to be intended to intimidate or coerce a civilian population; and to influence the policy of a government by intimidation or coercion.” If we substitute the word “corporation” for “government” in the definition, we have a terror act intended to intimidate and coerce the Sony Pictures Corporation into ending distribution of the movie. While we can’t say with certainty that the Sony hack was actually an act of terror, the event may have validated the idea that terrorism in the cyberdomain can be successful.

“Conventional wisdom holds that Russia hacks primarily for financial gain. But equally credible is the belief that the Russians engage in cyberwarfare to further their geopolitical ambitions.”

The Russian Federation holds an interesting, albeit a dubious position in the ranks of nation state cyber actors. While ranked third among countries in terms of volume of cyber activity (behind the US and China, according to Deutsche Telekom’s honeypot network data), Russia is widely regarded as a having the most sophisticated and skilled hackers.

Unlike the Chinese government which employs thousands of hackers in the People’s Liberation Army, the Russian government’s relationship with resident hackers is much murkier. The trails to cyber attacks originating in Russia tend to end at civilian hacktivist groups and criminal organizations, perhaps providing officials with plausible deniability. This may suggest an implicit support for criminal hackers in Russia, given government’s notorious reputation as being inherently corrupt.

Given the highly publicized industry hacks attributed to Russian entities, it’s easy to conclude that the government’s motivation behind hacking is directly related to financial gain. But that conclusion is, perhaps, somewhat simplistic. As an alternative, consider viewing Russian hacking through the prism of geopolitics. It is feasible that the Russian government has established an iniquitous partnership with Russian civilian hackers to achieve geopolitical goals. It may not be possible to know with certainty what motivates the government to participate in nefarious cyber activity, but it’s equally conceivable that Russian officials view hacking, or more appropriately cyber warfare, as a political tool which, when employed, is extremely effective at helping a nation state achieve a geopolitical goal.

The notion that the Russian government is willing to use the cyber domain as a political, if not military, arena is not new. Recall the cyber attacks alleged to have been orchestrated by the Russian Government during the 2008 Russo-Georgian War, a war considered by some to be the first cyber war. Post war analysis suggests that the Russian Government leveraged the vast network of civilian cyber actors, including organized crime organizations, to conduct the attacks. The military significance of the cyber targets attacked during the war, and the synchronization of the attacks with Russian military operations, may be too coincidental to reasonably conclude Russian civilian hackers were acting autonomously.
In December, the German Federal Office for Information Security (BSI) disclosed that a cyber attack was executed on a steel plant, resulting in the abnormal shut down of a large blast furnace and associated systems. The BSI report characterized the attackers as highly skilled, and that they used social engineering and extensive knowledge of the network to circumvent security and specialized software designed to prevent such attacks. It is difficult to identify with certainty the parties responsible for these attacks, but the timing of diplomatic talks between the Ukraine and Germany point toward the Russian government. This cyber attack is significant because it signals an escalation in tactics: a willingness to create physical damage to infrastructure.

More recently, the shutdown of German Government websites, which overlapped with a scheduled meeting this month between German President Joachim Gauck and Ukrainian Prime minister Arseny Yatseniuk, strongly suggests a connection between cyber operations conducted by Russian hacker groups and Russian politicos. The Russian hacktivist group, CyberBerkut, claimed responsibility for the attacks and demanded the Germans withdraw support for Ukraine. We can't be certain that CyberBerkut was sponsored by the Russian government, but the timing of the cyber attacks with Russian activity in the Ukraine is compelling.

The renowned German military theorist Carl von Clausewitz believed war to be a political instrument, and we can easily extrapolate Clausewitz’s thought to cyberwar in a modern context. The Russian government has applied Clausewitz’s theories to achieve national political goals by leveraging an increasingly sophisticated hacker population. While the US and many of her allies grapple with the implications of conducting offensive cyber operations, the Russian Government is writing the first book on geopolitics and global cyber warfare.

- Iran -

“Iran is using its increasingly sophisticated cyber capabilities to minimize Western influence and establish itself as the dominant power in the Middle East.”

The timing of the invitation to address a joint session of the US Congress from Speaker of the US House of Representatives John Boehner to Israeli Prime Minister Benjamin Netenyahu couldn’t be better for a discussion on Iranian cyber capabilities. Putting internal US politics aside, the event represents a continuing effort by Netanyahu to alert the world to the dangers of a nuclear-armed Iran. As with Iran’s desire to attain nuclear weapons, its history of bad cyber behavior is part of an Iranian strategic effort to establish a hegemon in the Middle East.

To understand the motivation behind Iran's goal of regional dominance, it's helpful to consider the relationship between Iran and the United States, as well as Iran's relationship with its Islamic neighbors in and around the Arabian Peninsula.

A quick review of recent history reveals an extremely sensitive relationship between the US and Iran. Since the Iranian Revolution in 1979, Iran and the US have been in a constant state of diplomatic tension which has extended to a kind of military brinksmanship. Over the decades following the revolution, the US has maintained a visible and proactive military presence in the region, exclusive of the Iraq Wars, in order to demonstrate its resolve to keep the Persian Gulf (or the Arabian Gulf, depending upon your perspective) open to trade. At the same time, Iran has tried to demonstrate its dominance in the region by posing a constant threat to control, if not deny, access to the Persian Gulf. This aggressive relationship between the US and Iran has become a symbol of Western meddling in the region from the point of view of Iran. This perspective is similar to China's view of the US presence in East Asia, although, in my opinion, the Chinese context is more related to economics. The Iranian perspective is partly economic as the country has a rich supply of natural resources (e.g. oil and natural gas). But it is also impacted by theology, the second motivation behind Iran's cyber activity.
Shifting Demographics

Islamic demographics in the region can be a little confusing, particularly as we watch the evolution of the Islamic State in Syria and Iraq. Until the rise of Al Qaeda and now ISIS/ISIL, Iran was the face of Islam in the Middle East. Ironically, the majority of the Iranian population practices Shia Islam while the majority of Muslims globally practice Sunni Islam.

The distinction is significant because enmity between the two sects is one of the root causes of the persistent tension in the region. Historically, the Sunni Islamic countries like Saudi Arabia, Kuwait, Jordan, Egypt, and Iraq before the first Gulf War, have been aligned with the West (represented by the US) both economically and militarily. Those alliances have created tension between Iran and its Sunni neighbors. We have seen that tension manifest itself as Iran continues to extend its influence in eastern Iraq and Yemen.

If Iran is to successfully establish itself as the dominant power in the Middle East, it must minimize Western influence in the region and increase its influence over its neighbors. To do that, Iran must disrupt the military and economic influence of Western countries that maintain a presence in the region, and at the same time it must destabilize those regional Sunni governments friendly to the West. As Iran continues to leverage the threat of nuclear weapons in the kinetic world, it is actively converting threat to action in the cyber domain to achieve its regional objectives.

Until recently, Iranian cyber capability wasn’t considered particularly exceptional. But shortly after the Stuxnet attack, largely attributed to the US and Israel, Iran initiated a focused effort to ramp up its cyber capability. Some experts believe that Iran has closed the cyber capability gap with countries like the US and Russia. The recent Cylance report on Iranian cyber operations identified a number of nations against which Iran has successfully conducted cyber espionage and/or established persistent presence in networks related to critical infrastructure and key resources (CIKR). Interestingly, China is on the list along with a number of US allies including Canada, Saudi Arabia, Qatar, Kuwait, and the United Arab Emirates, to name a few. Note the focus on Sunni states friendly to the US.

The North Korean Connection

Lest we believe that Iran operates in the cyber domain with pure strategic intentions, we should also note that like North Korea, Iran lashes out in response to perceived insults by conducting cyber attacks on alleged offenders. Iranian activists are reportedly responsible for a destructive attack on Las Vegas Sands Corporation in February 2014, in response to CEO Sheldon Adelson’s comments about detonating a nuclear bomb in Iran.

At the risk of appearing cliché, ‘axis of evil’ states tend to flock together. In September 2012, Iran signed an extensive cooperative technology agreement with North Korea. The partnership provides an opportunity for collaboration on information, security and development of technology programs between the two nations. The technology agreement, coupled with focused attacks on CIKR in South Korea by Iran, strongly suggest a cyber
alliance with North Korea. This partnership may also explain why the relatively unsophisticated North Koreans were able to carry out such a devastating attack on Sony Pictures.

- Israel -

Israel's tenuous position in the world drives its leaders to stay ahead of its cyber adversaries, among them the Islamic Republic of Iran.

Israel's intelligence corps, Unit 8200, has rapidly grown into one of the world's most formidable cyber counter-terrorism organizations. The elite group employs Israel's best and brightest to combat existential threats to its national security in the cyber domain. The number of nations and terror groups that threaten Israel is considerable, and the significance of the threat varies from political posturing, to a credible threat of harm to Israel as a nation and their people.

To understand how Israel has found itself in an adversarial relationship with most of its neighbors, it is useful to review the evolution of Israel as a nation. Admittedly, the history of modern Israel and its relationship with the Arab world is exceptionally complex. With that, the following is a brief summary intended to provide some historical context; it is not in any way intended to be comprehensive.

A Brief History

Beginning with the Zionist movement toward the end of the 19th Century, European Jews began migrating to Palestine in response to a growing tide of anti-Semitism. A number of events occurred in the first half of the 20th Century that would keep the growing Jewish community in Palestine on course toward achieving an independent Jewish State. The carefully crafted language of the Balfour Declaration of 1917 endorsed the creation of a Jewish "Homeland" in Palestine. The British Mandate for Palestine, authorized by the League of Nations in 1922, provided guidance for the establishment of a Jewish "Homeland" in Palestine.

The massive migration of Jews leaving Europe following World War II stemmed from suffering years of brutality at the hands of Nazi Germany and decades of enduring systemic patterns of anti-Semitism across Europe. These events contributed to a growing distrust of Zionists, and the nations that supported them, among Palestinian Arabs. The escalating tension between the two groups reached a tipping point with the end of the British Mandate in May of 1948, followed immediately by the Zionists declaring an independent Jewish State, Israel.

Although Jews and Palestinian Arabs had been actively engaging in hostilities during the period leading up to May 1948, the declaration triggered a broader conflict, with Egypt, Syria, and Jordan joining forces with Palestinian Arabs against the newly formed nation of Israel. The ensuing "War of Independence," or "al-Nakbah" ("the Catastrophe") as it was referred to by Palestinian Arabs, lasted just nine months, ending in armistice and with Israel intact territorially. Interestingly, land originally identified by UN Charter as territory designated for an Arab State, was divided among the three Arab nation signatories of the armistice, but it did not include the Palestinian Arabs.

Enmity between Palestinian Arabs and surrounding Arab nations continued to grow through the decades following the War of Independence, as the two sides fought for territory during the 1967 and 1973 Wars. But the fight was not contested in a geopolitical vacuum. Before the establishment of the State of Israel, the world's super powers, and their associated allies, began to polarize into pro-Israeli and pro-Palestinian partnerships. The US and its allies were generally allied with Israel. To counter US influence in the region, Russia gravitated toward Arab nations that held anti-Israeli positions.
WHY NATIONS HACK

The US-Israeli alliance, which includes an estimated as $121 billion in military and economic aid since World War II, is the foundation for anti-American sentiment throughout the Middle East and the Muslim world. Animosity toward both countries is still pervasive in region, but some Arab/Muslim nations have at times taken a more conciliatory tone toward Israel, examples of which include the Camp David Peace Accords between Israel and Egypt in 1979, and the Israel-Jordan Peace Treaty in 1994. Not so with Iran.

Enter Iran

Since the Islamic Revolution in 1979, Iran has expanded its sphere of influence in the Middle East. Today, Iran has sent a clear and unambiguous message to the global community that it wants to dominate the geopolitical landscape in the region. To do that, Iran has waged a campaign against Western influences and continues to destabilize pro-US Arab nations either directly or through surrogates. Most alarming is Iran’s clearly stated intent to wipe Israel, the only non-Islamic state and sole democracy in the region, from the face of the Earth.

Israel has demonstrated a willingness to assert its national power against hostile nations or terrorist organizations on a number of occasions. The Israeli military launched incursions into Lebanon in 1982 and 2006 to squelch terrorist activity and most recently launched attacks against terrorist sanctuaries in the Gaza Strip in response to terrorist rocket attacks and kidnapping of Israeli citizens. But more relevant to the current geopolitical discussion, Israel has demonstrated a steadfast resolve against nations that threaten its right to exist with nuclear weapons. In 1981, the Israeli Air Force launched a daring attack against Iraq, destroying a nuclear production facility.

Israel’s resolve to deny nuclear weapons capability to aggressor nations has since extended into the cyber domain. In 2008, faced with an imminent threat of a nuclear-armed Iran, Israel allegedly participated in a cyber attack (Stuxnet) against Iran, destroying the programmable logic controllers associated with centrifuges used to produce weapons-grade uranium. The attack was a part of a broader strategy intended to disrupt Iranian nuclear weapons production, started during the most recent Bush Administration and carried on by the Obama Administration. These attacks, coupled with Iranian attacks against Israel have resulted in a sort of a quasi/cyber war between Israel and Iran.

The Cyber Battleground

Iran is alleged to have launched a number of cyber attacks against Israel, including attacks against the Tel Aviv Stock Exchange, El Al Airlines, First International Bank of Israel marketing websites, and attacks against the Otzar Hahayal and Massad Banks. In January 2009, Israel’s Internet infrastructure was attacked by at least 5 million computers in response to its military offensive in the Gaza Strip. The attack is believed to have been launched by hackers in Russia and sponsored by Hamas or Hezbollah, both Islamist terrorist organizations known to be heavily influenced by Iran. In 2012, Hamas called upon Palestinian software developers around the globe to attack websites in Israel. During that time there were reports of 44 million attacks intended to disable Israeli websites. Most recently, Israel encountered roughly 900,000 cyber attacks per day during the 2014 Gaza campaign, an increase of almost 90 percent when compared to normal cyber activity.
Israel’s tenuous position in the world drives its leaders to stay ahead of its cyber adversaries. In September 2014, Prime Minister Benjamin Netenyahu extended the breadth of cyber defense beyond national defense organizations by establishing a national authority for operative cyber defense. This new authority will have all of the responsibility required to defend the civilian sector from cyber threats and will operate alongside the Israel National Cyber Bureau which is charged with national cyber defense. Notably, the US has a similar construct in the US with NSA/US Cyber Command, Department of Homeland Security, the FBI and other government agencies, but our system may be less cohesive based upon the number of agencies involved in the effort.

With Israel Prime Minister Netenyahu’s upcoming address to the US Congress, we will likely hear him frame the Iranian nuclear threat to the US through the prism of the Israeli experience. He will make it clear that Israel will not wait until Iran has a nuclear weapon before acting to counter the threat. We can assume that cyber operations will continue to be a fundamental part of any campaign intended to deny Iran with nuclear weapons production capability. It will be interesting to see if the campaign is confined to the cyber domain, or if it will expand to include kinetic operations.

- The United States -

The United States operates in the cyber domain as a national entity for one simple reason: to protect its citizens. Like traditional notions of national defense, cyber operations extend across political, economic and military pillars of national power. But cyber operations are, in a sense, more complex because they affect the pillars of power more profoundly due to the speed at which they occur.

Consider how quickly the Allied Forces moved across Europe during World War II following the D-Day invasion on June 6, 1944. Within about a year, the allies coordinated a multi-pronged campaign attacking the German military on the ground, the economy from aerial bombardment of German industry, and politically by strengthening the Allies while simultaneously dismantling the Axis forces. Now consider the speed at which a modern aggressor nation could attack another nation’s military, economy, and political establishment through cyber warfare. With the right planning, a well-coordinated cyber campaign could be executed with an immediate impact and with the same devastating effects.

In spite of the insight into NSA operations provided to us by Edward Snowden, I am steadfast in my belief that US cyber operations are focused solely on national defense and that those operations do not include the exploitation of information for economic or financial gain. Moreover, the US government imposes strict limits on cyber operations through statutes and regulations, and holds agencies accountable for violations of those statutes and regulations through comprehensive political oversight.

This is not to say that there isn’t potential for abuse of power of agencies in the “cyber” national defense community and the political establishment. That potential certainly exists and could manifest itself should the wrong people ascend to leadership roles in government at the wrong time. For skeptical readers, I can only emphasize that my assessment is based upon personal observations made during my recent tenure in the Department of Defense cyber community. For this discussion, I’ll focus on the three organizations that contribute to the national security effort by confronting threats from aggressor nations: CIA, NSA and United States Cyber Command.

CIA Mission Statement

Preempt threats and further US national security objectives by collecting intelligence that matters, producing objective all-source analysis, conducting effective covert action as directed by the President, and safeguarding the secrets that help keep our Nation safe.

Cyber Operations in a nation state context, map directly to every aspect of the CIA mission statement. By collecting
intelligence and producing analytical reports, the CIA plays an important role in building the threat picture for the intelligence community. But CIA cyber operations are bounded by the guidelines of Executive Order 12333 and Title 50 of the US Code. EO 12333 restricts CIA operations involving US citizens in the United States, and Title 50 refers to intelligence agencies, intelligence activities and covert operations. Because CIA operations are clandestine, there isn’t a broad body of knowledge available to the public that demonstrates how the Agency operates in the cyber domain. But most recently we do know that the CIA was allegedly involved in Operation Olympic Games, a cyber campaign directed at denying Iran nuclear weapons capability.

**NSA Mission Statement**

The National Security Agency/Central Security Service (NSA/CSS) leads the US Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances.

Although the reputation of the NSA, courtesy of Snowden, has been tarnished both inside and outside of the US, it’s important to realize that this agency has a long and storied history of protecting the United States from the full spectrum of adversaries by leveraging superior technology throughout the electromagnetic spectrum. Prior to the age of cyber, NSA operated in the spectrum to collect and analyze signals intelligence across the globe. Although information related to NSA operations is limited because of security concerns, many operations find their way to the media but the stories are often based more upon speculation than hard facts.

Clearly written in the NSA mission statement is the task of enabling computer network operations, implying both offensive and defensive capability. From a practical standpoint the NSA is the functional leader of US computer network ops across government including the Department of Defense. There is a deep symbiotic relationship between NSA and the uniformed services, particularly the Navy. That link was formalized through CSS, the component of NSA responsible for providing cryptologic support to the Armed Services.

Like the CIA, NSA operations are highly classified and when aspects of an operation end up in the public forum, they are typically subjected to a tremendous amount of speculation. The end result is usually an interesting story loosely based upon opinion. But some accounts of NSA operations are compelling and simply make sense. Ronald Reagan’s decision to launch air strikes against Libya (Operation Eldorado Canyon) following the 1986 German disco bombing which, unfortunately, took the lives of at least 2 U.S Servicemen, was believed to be based upon critical signals intelligence provided by NSA.

**United States Cyber Command (USCC) Mission Statement**

USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.

In the information age, military operations are completely dependent upon information systems for myriad reasons ranging from command and control of operational forces in the battlespace, to weapons systems, to everyday business of running the Navy, Army, Air Force and Marine Corps. That dependence was the motivation behind the establishment of the United States Cyber Command in 2009.

As Director of NSA, General Keith Alexander was the driving force behind the creation of an organization dedicated to supporting US Combatant Commanders in the field. General Alexander knew that the US military needed a unified force of cyber operators which could operate with the warfighters in the uniformed services, as well as with agencies like NSA. The connection already existed from an administrative standpoint, but there was no operational link with NSA. The distinction between operations and administration is significant because
WHY NATIONS HACK

the US government, particularly DoD, correctly views cyber space as another warfighting domain, akin to air land and sea. The bond between NSA and USCC was solidified with the dual responsibility of the Director NSA and Commander USCC.

The cyber army that General Alexander envisioned is taking the form of a Cyber National Mission Force of roughly 6,000 military personnel. The force, which will be distributed across 133 teams and is on track to be fully functional by 2016, will focus on three areas: providing support to Combatant Commanders across the globe, defense of the DoD information network, and protection of the nation’s critical infrastructure and key resources.

**Why The US Hacks**

When we look at all of the nations which we have discussed in this series, it isn’t surprising that the common answer to the question of “Why they Hack” is national defense. But to assume that national defense has the same meaning to different governments is overly simplistic. While we understand, intuitively, what a literal defense of a nation commonly means, the behavior of some nations in the name of national defense is difficult to explain.

We see China and Russia engaging in exploitation of intellectual property for economic and financial gain. We see Iran and China conducting cyber operations in an effort to expand their spheres of influence. We see North Korea lashing out in an effort to demonstrate its relevance in the geopolitical community. Finally we see Israel and the United States conducting cyber operations to protect their national security.

Does this mean that the United States and Israel maintain higher ethical standards of cyber conduct? I believe the United States does, but I admit that the point is arguable. We know that the United States has made mistakes; the Snowden data suggests that it did. But in the end, US cyber operations are bounded by laws, regulations and accountability, and that’s the only way to maintain order in an environment rooted in disorder.

**-About The Author-**

Mike Walls is a Retired Navy Capt and Naval Aviator with over 28 years of experience in Cyber and Aviation Warfare. While on Active Duty in the US Navy, Mike served as Commander of Task Force 1030 reporting directly to the Navy’s Fleet Cyber Command, and was responsible for Cyber readiness of over 300 ships, 4,000 aircraft and 400,000 people. He is a combat veteran of Operations Desert Storm, Iraqi Freedom and Enduring Freedom.

Mike is a 1986 graduate of the U.S. Naval Academy where he earned a Bachelor of Science Degree in Physical Science, and a 1996 graduate of the Naval Postgraduate School where he earned a Master of Science Degree in Operations Research. Since retirement from the US Navy Mike has served as Managing Director, Security Operations and Analysis with EdgeWave, a leader in cyber security. His weekly blog can be read at blog.edgewave.com.