# DEFENDING A NATION IN CYBERSPACE: A COLLECTIVE DEFENSE APPROACH

Gregory Conti, IronNet
Robert Fanelli, IronNet

## Introduction

Defending a nation in cyberspace is a difficult, but vital undertaking. In the physical world, strong borders and a robust military provide sufficient protection. However, in cyberspace borders are porous and attacks far more difficult to detect and mitigate. Cyberspace conflict occurs daily on a digital battlefield that also contains vast amounts of legitimate activity that fuels day-to-day commerce, the functions of government, and the lives of citizens. While defending a nation in cyberspace is difficult, it is possible to make rapid progress and greatly improve the cyber defenses of a nation.

As the Internet and Web grew, governments and businesses around the world quickly discovered the speed, efficiency, and cost savings of networked computing and raced to replace expensive manual systems with faster, cheaper automated systems. Dependency on automation soon followed. Over time, and through many painful lessons, leaders realized these systems possessed a fundamental flaw – each was vulnerable to attack. Interconnectivity, often touted as a benefit, made long distance, large scale, and highly disruptive attacks possible.

Where early attacks were a nuisance, the situation grew rapidly worse. *Today it is possible to systematically dismantle entire countries via cyberspace operations.* We have seen precursor efforts in Ukraine, Estonia, and Georgia, highly effective information-based attacks in the United States, the United Kingdom, Europe, and the Middle East, attacks across the U.S. financial sector and other critical infrastructure sectors, and destructive attacks against individual companies like Sony Pictures, Sands Casinos, and Saudi Aramco, among numerous others. Destructive attacks will only increase in intensity and frequency.

Based on history, many leaders think destructive attacks won't happen; they don't see the urgency. In this paper we illustrate what is in the realm of the possible. We are seeing acts rapidly moving from collecting information to disruption to destruction. Cyberspace operations are now a form of warfare and entire nations are at risk. Leaders have to understand the risks in order to defend their people, commerce, and way of life. We need to take steps as soon as possible.

The power to conduct highly destructive cyber attacks rests in the hands of multiple states and the cyber forces they enable. An attack could be a strategic move by a superpower, the result of a tyrant's tantrum, or something in between. Some think that cyber security is an *individual* organization's concern, each enterprise should stand alone against state threat actors. The government should protect itself. Companies should protect themselves. This is not true.

Governments must protect their country and its interests in cyberspace, just as they do in the physical world.

A devastating cyber attack should never happen, but we aren't taking the steps to prevent it.

There are no easy answers to cybersecurity, but we do know a collective defense strategy is the necessary foundation. Only a whole of nation approach can overcome the asymmetric advantage sophisticated cyber forces enjoy. Government is central to a country's cyber defense. It must provide the necessary resources, leadership, strategy, and legal authorities, else a piecemeal and ultimately indefensible security posture will result.

In this white paper, we outline solutions for protecting a country in cyberspace. We aren't going to rehash well-worn tropes like "defense in depth" or suggest a single security technology provides a perfect solution. The true answer requires a collective approach that brings together the government, the private sector, and individual citizens in defense of their country alongside well considered security technologies. We'll begin with illustrating what an attack might look like, then provide tools and techniques for understanding how a given country could be attacked, and then provide a series of actionable solutions.

## Cyber Effects and What They Mean for a Country

Individual cyber operations cause effects on their target, ranging from very subtle to highly destructive. When combined and carefully orchestrated, cyber operations can systematically undermine the people, processes, and technology that make a country viable. Civilization is fragile and it doesn't take long for a country to collapse if the population lacks power, food, communication, government leadership, and access to money.

Complexity is the bane of cybersecurity and today's computing systems are complex, beyond the capability of humans to fully understand. The result are flaws that attackers exploit to gain access to systems. Our adversaries work tirelessly to gain access to critical systems required for governments and businesses to operate, often with great success. This access may be used to conduct surveillance of their targets – gathering intelligence in anticipation of a future conflict and for day-to-day competition. When desired, adversaries can easily pivot from passive surveillance to aggressive attack, destroying systems and altering data, that can disrupt and destabilize countries, possibly even toppling governments. Systems are not isolated, but instead highly interconnected. The resulting interdependencies mean attacks on one system impact numerous others, often in unpredictable ways.[1]

Sometimes systems and protocols are functioning as designed, and unauthorized access isn't even necessary to have desired effects. Consider major social media sites which share information at high speed to millions of participants worldwide. Threat actors use fake online identities and news stories

[1] See Frederic Petit et al, "Analysis of Critical Infrastructure Dependencies and Interdependencies," Argonne National Laboratory, U.S. Department of Energy, 2015. https://publications.anl.gov/anlpubs/2015/06/111906.pdf

to fuel divisive tensions and strike fear in populations. Even cruder, and equally difficult to prevent, attacks are possible. Simply making a system available for shared use means it can be attacked. For example, web servers, by design, accept requests from many users to share information and process business transactions. Attackers can disrupt these systems by generating high volumes of spurious requests which slow or crash their target, like a major government or ecommerce website.

## Types of Effects

Attackers will develop offensive techniques, create battle plans, and systematically probe the critical infrastructure of their target, often years in advance. When the time is right, they will execute operations in support of a desired end state, like forcing a major concession from an adversary, acquiring valuable resources, or taking over a bordering county. Here are examples of cyber effects a state attacker might use in support of these outcomes.

**Isolation** – By combining physical destruction, cyber attacks, and electromagnetic spectrum jamming, attackers can isolate a target country making it difficult to request help from neighboring countries, the United Nations, or the rest of the world. Example targets include: undersea cables, orbiting satellites, satellite ground stations, internet routing infrastructure, members of the press, radio and TV stations, and cellular service providers.

**Deception** – Information operations make it difficult to distinguish fact from fiction. Propagated by social media, online videos, text messaging, radio broadcasts, and analog techniques like posters and leaflets, information operations hamper national command and control, frustrate international assistance, and destabilize the population – imagine using a realistic, but fake, video of a president telling his military to surrender.[2] Information operations are enhanced by cyber operations which reach into networks to steal, alter, or plant information or deny access to true information.

**Energy Interruption** – Electricity is the lifeblood of modern civilization. Attackers can interrupt power generation and transmission, immediately disrupting day-to-day life, business transactions, law enforcement, and emergency medical care. Disruption could be temporary, but if the attacker desired, can be made long-term by destroying hard to replace components that take months, or even years, to replace.

**Transportation Disruption** – Most cities would last only a few days with the day-to-day supplies they have on hand. Attackers can disrupt fuel shipments, food deliveries, relief supplies, the movement of military forces, and the exodus of refugees, creating an impassible snarl of congestion on all forms of transport.

**Financial Upheaval** – Business today is dependent upon digital transactions, whether it is buying milk at a grocery store, trading stock, exchanging currency, or transferring large sums of money between banks. By disrupting financial systems, attackers prevent citizens from making purchases, destabilize fiat currency, cause a run on banks, or crash a stock market.

[2] Kevin Kelleher, "What Is a Deepfake? Let This Unsettling Video of Jennifer Lawrence With Steve Buscemi's Face Show You," Fortune, 31 January 2019. http://fortune.com/2019/01/31/what-is-deep-fake-video/

**Degrade the Military** – Military forces are what keep a country safe from adversaries and hence are a prime target for attack. Cyber operations can directly attack weapon systems making them unreliable, prevent generals from communicating with their troops, or even demoralize service members by sending threatening text or social media messages to them or their families.

**Frustrate Government Function** – Cyber operations can wreak havoc in government function. In a crisis, leaders would not know the current situation and would lack the ability to communicate with subordinates to provide response, while the pillars of society – law enforcement, fire departments, taxation, commerce, courts, medical care, etc. – break down, threatening the legitimacy of the government itself.

These are just a few examples of many. Individually, all of these examples are damaging, but when used in combination, the combined effect is devastating, see Figure 1. Known and unknown interdependencies, in and between systems, will magnify the havoc even further. Expect critical systems to fail, data to spill, and the information environment to be murky. It would not take long to destroy the integrity of an entire country. We understand these individual scenarios are not pleasant, but a reality – sadly, without proper defenses this is a predictable outcome of our dependence on technology.

Let's now look at how these and other cyber effects would be combined in full-on attack against a country and how we might create suitable defenses.

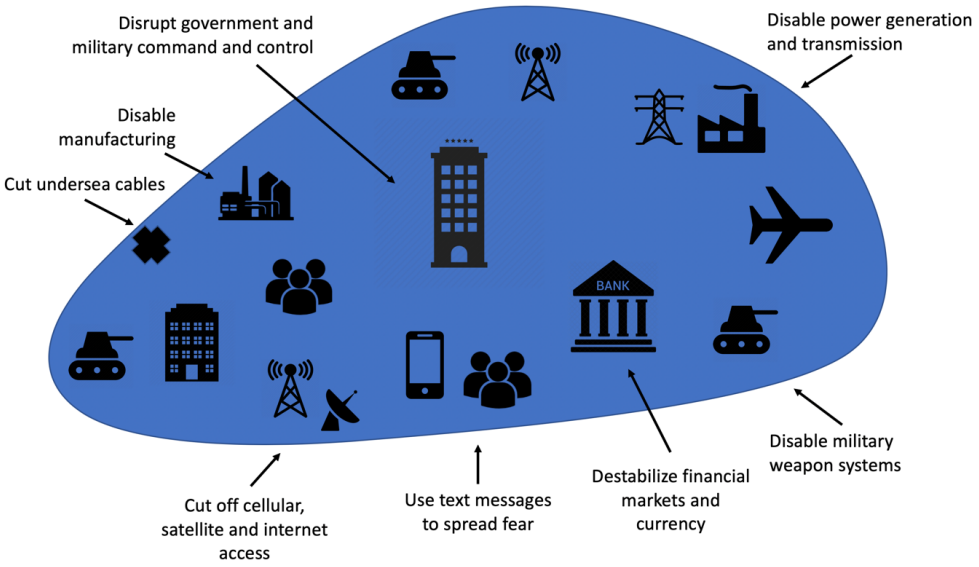


*Figure 1: Attacking an example country using cyberspace operations on multiple fronts. Attackers will seek to disable, degrade or destroy government and military command and control, military weapons systems, power generation and transmission, and banking and finance.*

## Case Study: Protecting a Nation in Cyberspace

There is no single way a country may be attacked, but the following demonstrates what an attack might look like and lays the foundation for a better defense.

### Prior to Hostilities

Attacks begin with substantial preparation, often years in advance, to understand the target, where it is vulnerable, and where it can best be influenced. Adversaries will conduct reconnaissance, gain access to important systems and people, and conduct operational planning, all while seeking to avoid detection. See Figure 2.

Attackers will probe defenses, systems, infrastructure, trust relationships, and people looking for weaknesses that can be exploited. This phase will include gathering information from social media accounts and freely available information.

Where possible, attackers will compromise systems and people to access confidential information and gain influence that might be exploited in time of conflict, or even prior to conflict, as part of international competition. Examples include using fake online identities to build relationships with important individuals like senior leaders and well-placed engineers (and their families), compromising the hardware and software supply chain, acquiring user passwords, and inserting intelligence operatives into target organizations, among numerous other strategies. Here the attacker, slowly and unobtrusively chips away at the target country's defenses.

Expect the adversary to patiently wait for an opportunity to gain access, even if there is only a few minutes of vulnerability on a single Saturday night at 3am once a year. By combining knowledge gained via these activities, military planners will construct and refine war plans that provide a roadmap of actions to take in time of conflict. Even if hostilities ultimately do not occur, adversaries will use the information gained to further their political, economic, and social aims.

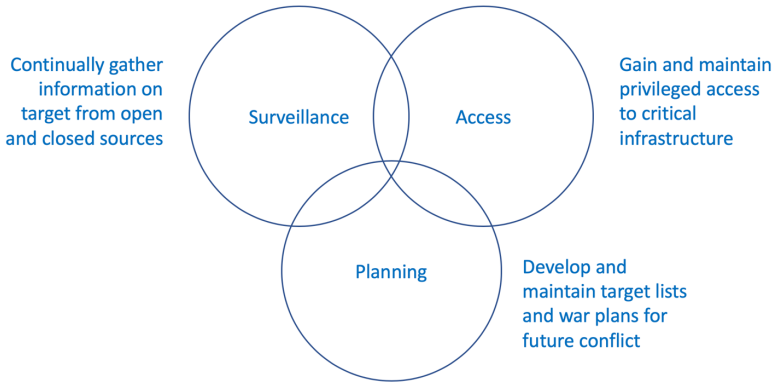


*Figure 2: Prior to hostilities attackers will continually surveille target countries, seek to gain access to key systems, organizations, and people, and develop operational plans for future use.*

## Escalation of Hostilities

As the situation worsens, adversary leadership will determine what cyber tools, techniques, and forces might be used to accomplish the desired end state. War gaming will vet and refine the plans and mature a preferred strategy.

Here is one potential strategy for a cyber attack on a notional country as it reaches a point of deliberate escalation. See Figure 3 for a graphical depiction.

1. Begin the attack with a false flag operation that blames the government for an atrocity it did not commit. Share videos via social media for internal and external consumption. Tell audiences the government is going to disrupt their access to cellular and mobile internet systems to hide their evil government activities.
2. Temporarily take down cellular service and mobile internet access as show of force to demonstrate capability and intent to leaders and sow fear in population.[3]
3. Make initial demands of target country's leadership, stop if met. If not, then escalate further.
4. Cause disruption via on-net hacking of financial, government, industrial, air traffic control, and military systems. Power, internet access, and the recently restored cellular service have deliberately not been affected to facilitate remote hacking efforts and to allow dissemination of deceptive news reporting.
5. Send threatening text messages to the cell phones of senior leaders and their families. Release a fake presidential video encouraging citizens to welcome the aggressors as friends and saviors.
6. If demands are not met, escalate to more destructive attacks.
7. Severely disrupt cellular phone access and destroy cell phones if possible.
8. Disable ISPs to prevent citizens from accessing the internet.
9. Cut undersea cables and disable satellite ground stations to isolate the country virtually.
10. Destroy network routers and other infrastructure to prevent bringing services back online.
11. Take down the power grid and leave the population in the dark.
12. Make further demands of target country's leadership using radio and increase pressure via other levers of power (e.g. diplomatic, economic, and kinetic military operations, etc.) until full demands are met.

Note that attacks must be carefully synchronized and sequenced. For example, you cannot send text messages to leaders unless cellular infrastructure is functioning, remote hacking efforts require power and internet access, and government leaders cannot communicate unless they are left a means to do so, such as satellite phones or radio transceivers. Additionally, attackers can selectively target infrastructure to herd their targets onto other desired networks, such as compromising email systems to encourage more cell phone use.

[3] For more information on show of force, see https://en.wikipedia.org/wiki/Show_of_force.

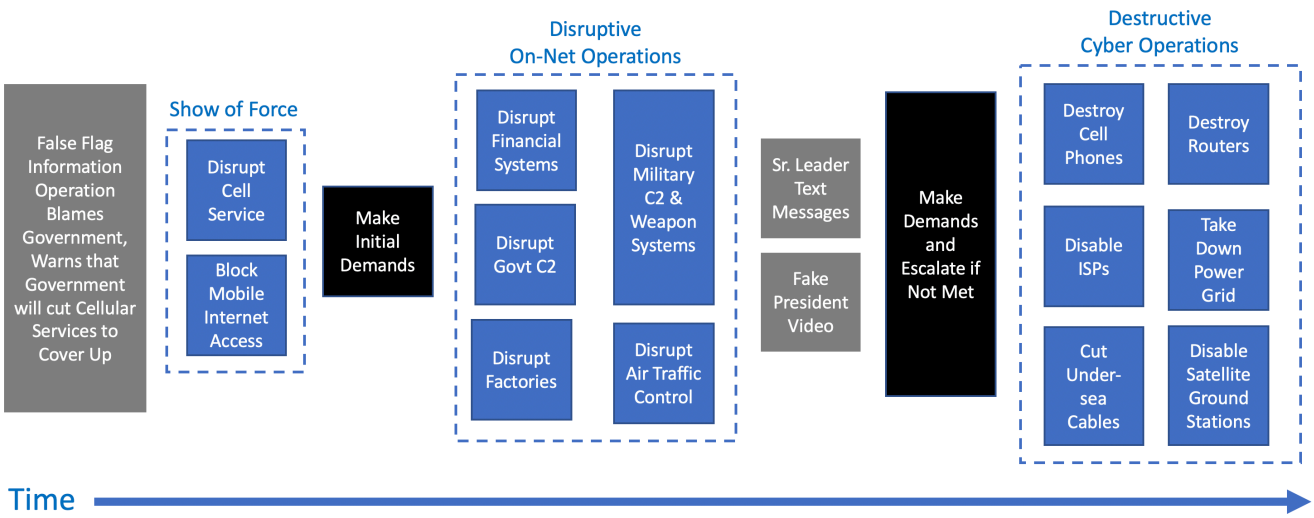


*Figure 3: Example attack on a country. Note that the conflict begins with a show of force and initial demands. If the demands are not met, the attacker increases pressure through a series of disruptive and destructive cyber attacks. A disinformation campaign occurs throughout.*

## Steps to Secure a Nation

We just illustrated what an attack might look like. Let's examine how to prevent such an attack.

### Create a Sense of Urgency

The most important thing for defending a nation in cyberspace is a sense of urgency. *Senior leaders must first recognize the need for cybersecurity, make cybersecurity a priority, and step forward as a champion of the cause*. These leaders must then communicate this sense of urgency across the breadth and depth of their organizations. Senior leaders can hold subordinates accountable for progress or the lack thereof. Without senior leader champions, well-intentioned initiatives at the lower levels can often wither and die. With top-level support and attention, however, cybersecurity can improve dramatically. If senior leaders think that cybersecurity will not be important until threat actors create highly visible physical effects, then those who attempt to construct defenses face an uphill battle and these problems won't be addressed until the real-world consequences are much too dire.

### Ensure Fundamental Defenses are in Place

After gaining top-level support, leaders should seek to implement the fundamental components of cyber defense. An excellent place to start is the Center for Internet Security's (CIS) Top 20 Security Controls[4] and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[5] By implementing the CIS controls and the NIST framework, organizations can defend against about 80% of cybersecurity threats. Progress toward implementation and long-term continued maintenance should be captured and reported to senior leaders on a regular basis to drive momentum and ensure compliance. Lack of senior leader interest will stall progress; fundamentally leaders need to create a culture where security is integrated into all efforts from the beginning.

[4] Center for Internet Security, "CIS Controls," https://www.cisecurity.org/controls/.
[5] National Institute of Standards and Technology, "Cybersecurity Framework," https://www.nist.gov/cyberframework.

## Defend as a Team

Standing alone when it comes to cybersecurity all but ensures being defeated individually. Successful defense of an individual organization—much less an industry or nation—fundamentally requires a team effort. State and state-enabled actors possess resources that far outmatch those of individual public and private groups. Indeed, bringing together the relevant players across government, law enforcement, the military, the intelligence community, and the private sector onto the same team maximizes one's capabilities and minimizes the waste of resources. This is true whether one builds a cyber defense team in an individual organization, in a military service, in a critical infrastructure sector, as a city, or as a nation.

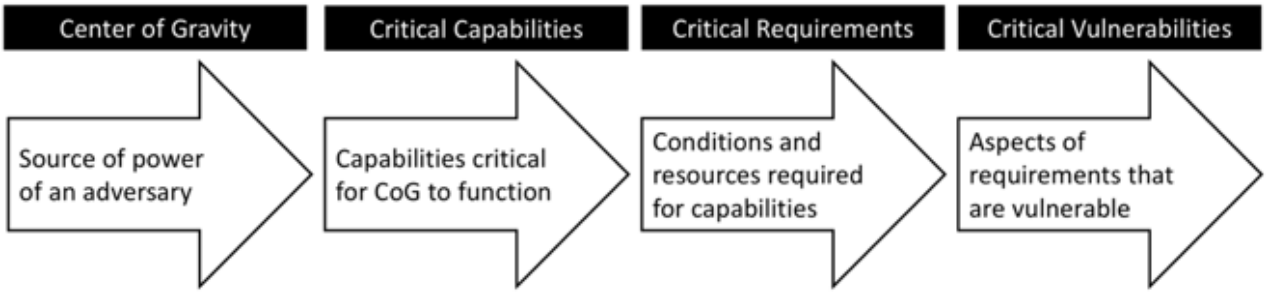


*Figure 4: Center of Gravity analysis helps organizations determine where they are vulnerable.*[6]

## Know How You Will Be Attacked

It is difficult to defend if you do not know where and how you will be attacked. A powerful means for understanding how you could be attacked is Center of Gravity (CoG) analysis (see Figure 4).[7] CoG analysis can break down any entity – be it a country, a critical infrastructure sector, an organization, or even a household – into its constituent parts to determine points of vulnerability:

1. *Center of Gravity* – Identify the key asset or source of strength for the entity
2. *Critical Capabilities* – Determine the capabilities critical for that entity to function.
3. *Critical Requirements* – For each critical capability, identify the conditions and resources required for those capabilities.
4. *Critical Vulnerabilities* – Analyze each critical requirement and determine which aspects are vulnerable.

[6] Derived from Gregory Conti and David Raymond, *On Cyber*, Kopidion Press, 2017, p.186.

[7] See JP 5-0: Joint Planning, U.S. Department of Defense, 2017, p. IV-23 and Gregory Conti and David Raymond, *On Cyber: Towards an Operational Art for Cyber Operations*, Kopidion Press, 2017, p. 186. For an example of Center of Gravity analysis in the cyber context see Gregory Conti, "What Would You Do With a Nation-State Cyber Army?" USENIX Enigma, 2018 and Rock Stevens, Colin Ahern, Patrick Sweeny, and Michelle Mazurek, "The Battle for New York: A Case Study of Applied Digital Threat Modeling at the Enterprise Level," USENIX Security, 2018. For an overview of more tactical IT threat modeling approaches, see https://en.wikipedia.org/wiki/Threat_model.

The result of CoG analysis is a much deeper understanding of one's vulnerabilities, which can be used to develop actionable defensive plans. This implies you must know your own systems better than your adversaries.[8] Threat actors will apply CoG-like analysis to your organization as well, but instead of developing defensive plans they will use the identified vulnerabilities to create a targeting list, matching capabilities and assigning forces to exploit these vulnerabilities in order to achieve their objectives.[9]

When starting this analysis, it may make sense to think in terms of operational military domains: air, land, sea, space, and cyberspace, as well as the electromagnetic spectrum.[10] Each represents a means of attacking a nation directly or indirectly via cyberspace and cyber operations. At the national level, analysts should also pay particular attention to critical infrastructure sectors as these will be likely targets for attack.[11] However, other important systems and services should additionally be considered, whether part of a critical infrastructure sector or not.[12]

The cyber attack surface of a nation is complex. One way to manageably understand how you can be attacked is to conduct analysis using a planes model, see Figure 5. The lowest plane is the *Geographic Plane* where real-world entities reside: roads, bridges, buildings, data centers, and so forth. The next level is the *Physical Plane* consisting of computing hardware and the underlying requirements for networking: fiber optic cable, satellites, the electromagnetic spectrum, etc. The next level is the *Logical Plane,* sometimes called the *Virtual Plane*, where software, data, and network traffic reside. The next level is the *Cyber Persona Plane* which contains digital identities, social media, and user accounts. The final level is the *Supervisory Plane* where command and control (C2) takes place and human decision makers reside.

[8] Rob Joyce, "NSA TAO Chief on Disrupting Nation State Hackers," USENIX Enigma, 2016. https://www.youtube.com/watch?v=bDJb8WOJYdA. For example, not all organizations know how many devices they have, where they are located, their current patch level, and any known vulnerabilities they possess.
[9] See Effects Based Operations, https://en.wikipedia.org/wiki/Effects-based_operations.
[10] There is debate in military organizations whether the electromagnetic spectrum should be considered a formal war fighting domain. See Lauren Williams, "Navy Declares EMS a full-fledged warfighting domain," Defense Systems, 23 October 2018.
[11] The U.S. Department of Homeland Security recognizes 16 critical infrastructure sectors. See https://www.dhs.gov/cisa/critical-infrastructure-sectors.
[12] See Gregory Conti and Robert Fanelli, "Dim Mak: A Study on the Pressure Points that Could Take Down Cyberspace," BSides Long Island, January 2018.

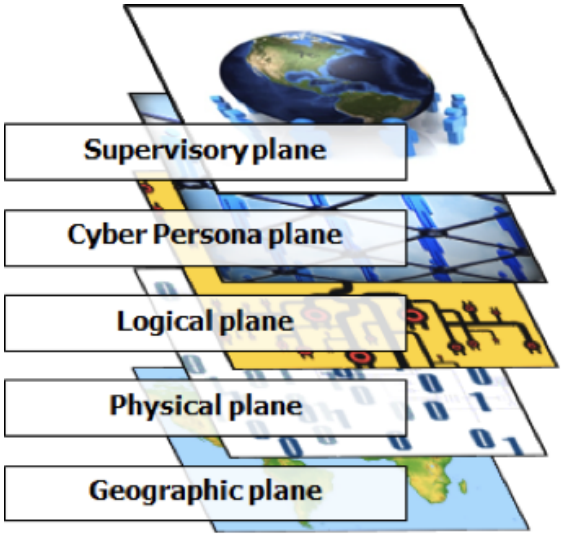


*Figure 5: Vulnerabilities exist on any plane. Attackers will exploit these vulnerabilities individually or in carefully synchronized combination to cause effects or for passive intelligence collection.*[13]

A nation's attack surface is a complex projection across all of these planes – and there will be many points of vulnerability. An attacker will seek to target these points of vulnerability, individually or more likely, in carefully synchronized combinations to cause serious impacts on the integrity and function of a nation. A nation should conduct their own analysis of these points of vulnerability *before their adversaries*, seeking to identify and secure those points that are most likely to be attacked or most dangerous if attacked. Sensors, security countermeasures, and intelligence assets should be placed along probable avenues of approach to give indications and warnings of looming or in-progress attacks. This analysis should include oft-overlooked vectors such as hardware and software supply chains, insider threats, and the electromagnetic spectrum.

State threat actors will amass and catalog these points of vulnerability and integrate them into their operational plans for causing negative effects on their adversaries at a desired time, either in support of information operations, other offensive efforts, or to conduct intelligence collection. A common model of this planning is shown in Figure 6, which illustrates how state actors look first at their desired end state, develop a list of targets (using techniques similar to those just described), determine what tools and techniques they will use, assign forces, conduct the mission, assess the results, and then begin all over again. Nations seeking to defend themselves must disrupt this cycle at multiple steps in the process.

[13] Derived from Gregory Conti and David Raymond, *On Cyber: Towards an Operational Art for Cyber Operations*, Kopidion Press, 2017, p. 69.

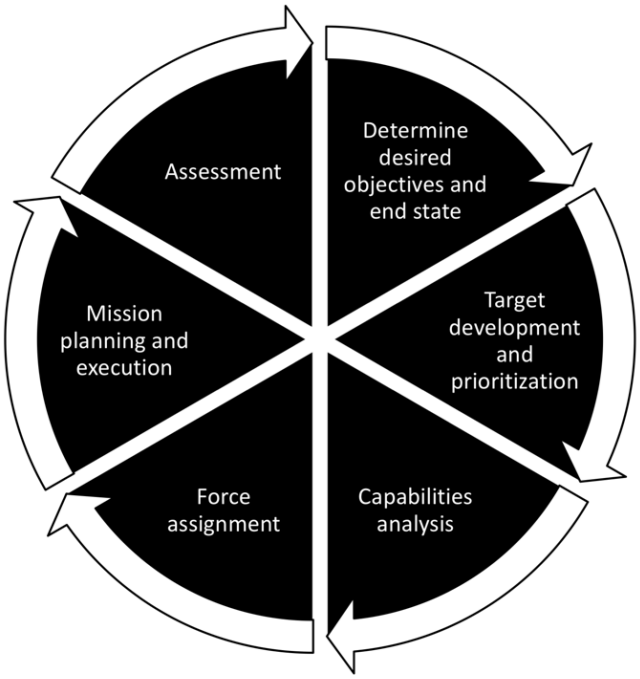


*Figure 6: State threat actors will marry the results of threat modeling with desired objectives to develop a targeting list that guides future attacks.*[14]

After conducting a national-level analysis, it is useful to conduct subordinate analyses, as needed, looking at entities such as individual cities, corporate ecosystems, and military organizations. Military organizations should analyze the IT infrastructure they use to store, process, and communicate information and, importantly, other technologies they employ, from GPS systems to night vision goggles to weapon systems. The results may be surprising.[15] The analyses we suggest will illuminate vulnerabilities and uncover surprising interdependencies. However, analysis alone will not win the day. It is critical that cyber defenders construct and implement defensive plans that utilize these results to close up the most critical vulnerabilities and get ahead of potential attacks before they occur. Doing so will allow defenders to be proactive rather than reactive.

## Know Your Adversaries

Knowing yourself, the assets you wish to protect, and how they are vulnerable is a great start but alone is insufficient – you must also know your adversaries. An essential part of national-level cyber defense is a robust collective cyber threat intelligence program that is built upon the foundation of national-level and military intelligence activities. This also includes, importantly, threat information sharing systems between government and the private sector. Such processes are essential for efficiently and effectively attributing attacks and leveraging the full spectrum of national power,

[14] Derived from JP 3-09 Joint Fire Support, U.S. Department of Defense, 12 December 2014, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_09.pdf.

[15] "Weapon Systems Cybersecurity, DoD Just Beginning to Grapple with Scale of Vulnerabilities," U.S. Government Accountability Office, October 2018.

including military operations, cyberspace operations, diplomatic actions, information operations, and economic sanctions to deter future attacks.

### *Employ Advanced Defenses*

The most dangerous cyber threat is the state actor. State-level cyber forces are patient, adaptive, tenacious, and well-resourced.[16] Traditional signature-based security systems will not catch their activities and other approaches are necessary. For example, we recommend using network behavioral analytics in combination with other tools, in order to look for the distinctive, hard-to-mask behaviors of these groups. Combined with network hunting and threat intelligence, behavioral analytics allow a defender to detect potentially new or previously-unknown or unnoticed malicious activities, attribute attacks to those responsible, and facilitate deterrence efforts. See Figure 7.

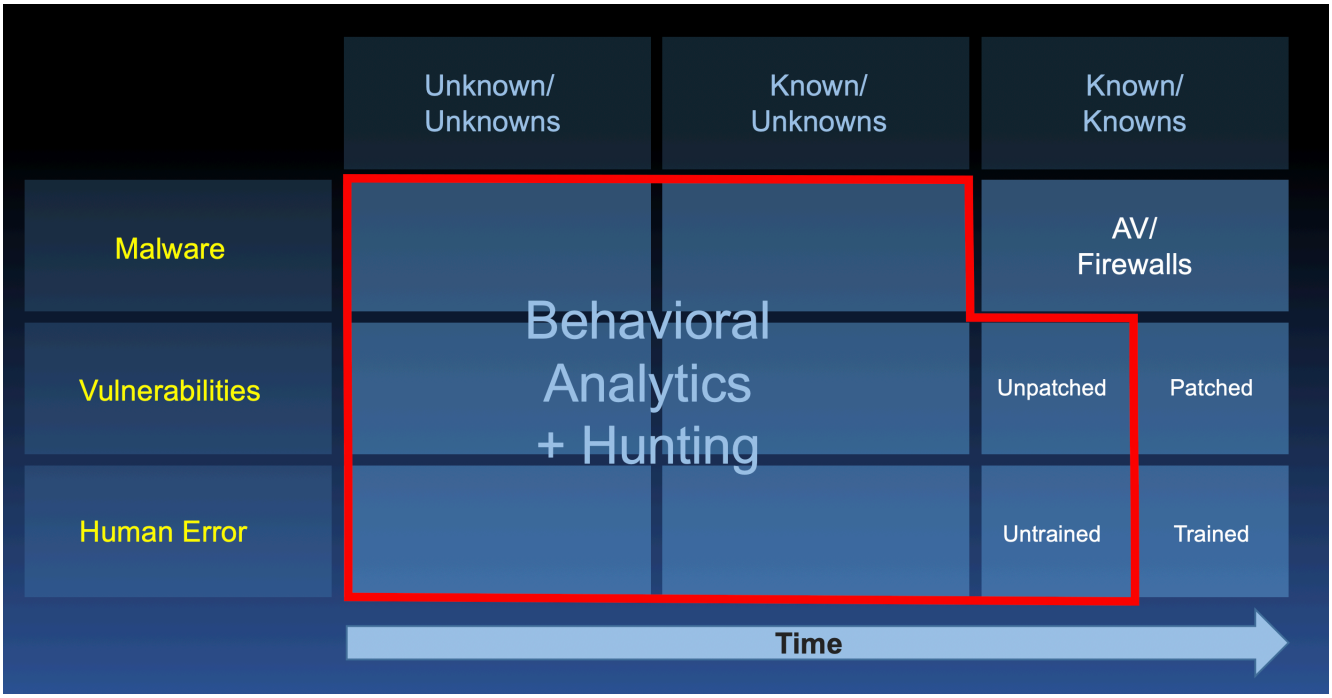


*Figure 7: Behavioral analytics combined with network hunting enables rapid detection of Unknown/Unknowns (novel 0-day class attacks) and Known/Unknowns (the general attack type is known, such as malware that jumps across air-gapped networks, but new instances are unknown) across the spectrum of malicious software, system vulnerabilities, and human error. Legacy signature- and rule-based systems, such as anti-virus and firewalls, aid against known classes of attack, vulnerability, and error.*

[16] See Gregory Conti and Robert Fanelli, "How Could They Not: Thinking Like a State Cyber Threat Actor," (to be published).

### *Emulate the Threat*

Knowing your adversary allows you to understand their thought processes and emulate their activities. Military forces have long employed opposing forces (OPFOR), such as those deployed at the U.S. National Training Center (NTC),[17] to give friendly forces an opportunity train against a realistic adversary. Employing simulated, but realistic tactics works to train cyber defenders as well. Military forces should organize and employ red teams to test their defenses and train their defenders. For example, we recommend using Cyber Threat Emulation (CTE) to emulate malicious software (malware) inside your network perimeter. By using CTE we have found that defender's assumptions about their cyber defense systems *always* differ from the reality.[18] Beyond testing defensive technologies and identifying additional ways to strengthen and harden one's cyber infrastructure, CTE is useful for testing incident response plans, the effectiveness of security event reporting, and the teamwork in Security Operations Centers (SOCs).

### *Maintain Situational Awareness*

To defend a nation in cyberspace also requires situational awareness of both friendly and threat forces and activities.[19] Your earlier analysis of threat avenues of approach and attack vectors provided insight into how you might be attacked. Without proper sensors, however, cyberspace is largely invisible. By deliberately placing sensors along the attack vectors you identified[20] and linking them with behavioral analytics and other key defensive systems, you can gain early warnings of when you are being attacked. Your intelligence teams can also develop Indications and Warnings (I&W) guides that help your SOCs and security teams identify attacks earlier.

### *Share Threat Information in Near-Real-Time*

A core component of situational awareness is threat information sharing. Without it, each organization has only a very limited view of the current threat picture. Speed is critical. In a crisis there is insufficient time to telephone a friend in another company. Near-real-time information sharing is essential. Threat reporting and contextual information from individual organizations, critical infrastructure sectors, cities, and the government should be aggregated and acted upon at a national-level SOC, which should include reporting from inside the military, law enforcement, the private sector, and across government, as well as from international sources.

## Develop the Cybersecurity Workforce

A qualified cybersecurity workforce in government and in the private sector is essential to defending a nation in cyberspace. Contrary to many opinions, *everyone* is part of this workforce. Even those far

[17] See https://en.wikipedia.org/wiki/Fort_Irwin_National_Training_Center for more information.
[18] See Ken Jenkins and Stuart McMurray, "Endpoint to Internet: Security Control Validation Using Threat Behavior Emulation," BSides DC, 2018. https://www.youtube.com/watch?v=WMDQOVy1nWM
[19] See Gregory Conti, John Nelson, and David Raymond, "Toward a Cyber Common Operating Picture," NATO Conference on Cyber Conflict, 2013 for more information.
[20] We encourage you also to place data collection sensors in Industrial Control Systems (ICS) for maximum visibility. Unwatched avenues of approach and attack surfaces are a recipe for a dangerously successful attack.

removed from hands-on-keyboard technical activities are still users of technology, and poor security practices at any level will create flaws in otherwise sound defenses. One approach for cybersecurity workforce development is to place people into three categories:[21] *the few* (those who specialize in cybersecurity), *the some* (those who conduct work in information technology (IT) and those who enable information security, such as cyber law professionals), and *the many* (the rest of the workforce) and plan training and development activities to give them the right amount of cybersecurity knowledge at the right point in their careers.

Cybersecurity specialists are in critically short supply. Military organizations and governments can make progress by identifying their members who already possess expertise in security and working to create viable career paths that will chain together individual assignments into a career-long experience that will grow true experts, rather than to have to fight an outdated personnel system. There is substantial demand for cybersecurity professionals in private industry and leaders should create a culture where these service members want to work, are rewarded appropriately, and feel valued, lest military organizations lose desperately needed talent, particularly to more lucrative private sector opportunities.[22]

## Military Cyber Defense

There are many military-specific aspects relevant to cybersecurity. We've mentioned the importance of monitoring threat activities, equally important is monitoring friendly activities – knowing where your information systems are located physically and virtually, as well as what users are doing – but this is often easier said than done. Organizing a military service to incorporate cyber operations is essential, but sometimes may conflict with the culture of traditional kinetic military thinking. Defending in cyberspace demands controlling and shaping the flows of information, both inbound and outbound. Operations Security (OPSEC) helps limit the flow of outbound truthful information, Military Deception (MILDEC) provides alternate realities to deceive the enemy, Counter Intelligence (CI) helps blunt the efforts of adversary intelligence collection, and Psychological Operations (PSYOP) provides a flow of tailored, but often truthful information to win over the hearts and minds of neutral actors and adversaries alike. All of these must be harnessed to thwart adversary operations.

Military operations must closely integrate cyber capabilities with kinetic operations. This includes conducting individual and collective training to exercise cyber capabilities in conjunction with traditional kinetic training.[23] Friendly forces will learn what is, and what is not, possible using cyber capabilities. Joint and combined exercises and war games which bring together diverse military forces alongside government, law enforcement, private sector, intelligence community, and international partners will help nations fight and defend efficiently and effectively. Perhaps more important, these

[21] The "many, some, few" model comes from work by a U.S. inter-service academy working group on cybersecurity education.
[22] Josh Lospinoso, "Fish Out of Water: How the Military is an Impossible Place for Hackers and What to Do About It," War on the Rocks, 12 July 2018.
[23] See Steven Stover, "Cyber Activities at the National Training Center Support Real World Operations," Army.mil, 7 February 2018.

events will lead toward shared trust, standard operating procedures, information sharing, interoperability, and common doctrine that will maximize teamwork.

Military cyber defense will require the creation of new military units, some of which may serve as strategic operational assets,[24] be integrated into kinetic warfighting organizations,[25] serve as training schoolhouses,[26] or even as service-level innovation centers.[27] However, creating new military organizations in general is consistently a difficult task, but is often more difficult for new cyber organizations. While kinetic organizations train to fight in a future war, cyber operators are engaged with adversaries on a day-to-day basis, so new cyber units must deliver real results even while they are still forming. Senior leader support is therefore essential to provide the resources necessary and prevent cannibalization or misuse by kinetic warfighting organizations or headquarters staffs.

Military doctrine for cyber defense is still evolving, but progress has been made. Rather than recreate new doctrine from scratch we recommend building upon work already done[28] as well as integrating emerging concepts.[29] Similarly we recommend the review of military service-level and national-level strategy documents and continuously updating and evolving your defensive approaches as new best practices and capabilities emerge.[30]

[24] See https://en.wikipedia.org/wiki/780th_Military_Intelligence_Brigade_(United_States)
[25] Caleb Minor, "New Space, Cyber Battalion Activates at JBLM," Army.mil, 16 January 2019.
[26] George Seffers, "U.S. Army Builds Cyber Branch One Step at a Time," Signal, 1 April 2015.
[27] Jeremy Bunkley, "SecArmy officially opens Cyber Institute at West Point," Army.mil, 10 October 2014.
[28] See JP 3-12 Cyberspace Operations, U.S. Department of Defense, 8 June 2018 as an example.
[29] See The Cyber Defense Review, https://cyberdefensereview.army.mil/, the proceedings of the NATO Conference on Cyber Conflict (CyCon and CyCon US), https://www.youtube.com/user/natoccdcoe/videos, and Gregory Conti and David Raymond, *On Cyber: Towards an Operational Art for Cyber Operations*, Kopidion Press, 2017.
[30] Examples include the U.S. National Cyber Strategy, 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf and the U.S. Department of Homeland Security Cybersecurity Strategy, May 2018, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_0.pdf.

## End State: National Collective Defense

In this paper we offered ideas for defending a country. By thinking holistically we can execute a series of steps that create a formidable defense. The desired end state for national-level cyber defense is a single, effective team that brings together the full spectrum of military, private-sector, government, intelligence community, and international capabilities for cyber defense. Defenders need to work together to counter threats. Cyber defenders are overtaxed by sheer volume and suffer skill gaps. As noted above, no organization, no matter how large, has the resources to stand alone against state threat actors. To stand alone is to be defeated in individually. Medium and small organizations are nearly defenseless in face of the increasingly complex threat landscape. Even large organizations are at a disadvantage against state threats. As a result, collective defense is an absolutely necessary strategy to cope with the present and future threat environment.

Cyber defenders must work together in common defense across logical groups to best gain broader situational awareness of the threats targeting their organization or sector and mitigate threats targeting the collective group. For a collective defense to work, sharing needs to be in near-real-time and across a broad base of indicators, risk-models or other resources where it makes sense. This way an attack on any of the organizations in the collective can and should be immediately shared and defended by all.

*We would like to thank the team at IronNet for their feedback and helpful ideas.*

*The views expressed in this paper are those of the authors and do not reflect the official policy or position of IronNet Cybersecurity, the United States Government, or any of our other current or past employers.*