Warfare and the Continuum of Cyber Risks: A Policy Perspective

Andrew CUTTS
U.S. Department of Homeland Security

Abstract. At the highest levels of national government, two of the most important decisions to get right are properly prioritizing among competing missions, and balancing between short-term and long-term objectives. The most consequential and highest risk threat is attack by one or more nation-states intent on projecting power, and who are willing to damage or destroy critical information infrastructure by cyber means in order to achieve this objective. Threat actors falling into this category have the necessary time, resources, sophistication, and access to do so. This category certainly includes cyber warfare. Today, nation-states are beginning to understand in concrete terms the potential benefits and costs of cyber attacks used as a means of projecting national power. It may not take a great deal of a nation's cyber resources, planning time, or technical access to achieve limited national objectives.

In the U.S., cyber defense of critical infrastructures is largely a homeland security mission. It may be that defense always lags the most potent offense. But the goal is an *effective* defense, not a perfect one. To get ahead of the most serious national cybersecurity risks, including that of cyber warfare, a country's cybersecurity leadership must seek an appropriate balance of resources, energy, and focus between those threats that are most frequent and those that are most consequential. The historical bias in dealing with cyber risk has been to look at it through the lens of commerce, not national security – and to reinforce the emphasis on short-term thinking rather than long-term strategy. One way to overcome this bias is simply to emphasize efforts that mitigate the most consequential risks. A nation's cyber leadership could decide, for example, that it should apply significant early resources to mitigating the national security risk associated with defending critical infrastructure against nation-state threats.

Keywords. Cyber warfare; critical information infrastructure; cyber risk; cybersecurity policy; cybersecurity; homeland security; cyber attacks

Author's note

This paper offers a framework for thinking about and debating vital national cybersecurity policy issues. It makes no attempt to settle those issues. Its primary purpose is diagnostic. To the extent it offers prescriptions, it does so only to forward thoughtful debate and discussion. It does not reflect a settled position of the Department of Homeland Security or of the U.S. Government.

Introduction

The cyber attacks against Estonian networks in 2007 were a wake-up call for information-based societies in general, and for the North Atlantic Treaty Organization in particular. Those attacks demonstrated that protecting classified networks and defense-related communications, while very important, is insufficient for an information based nation-state.[1] They forecast the risk that critical information infrastructure owned and operated by the private sector, including that which supports energy, transportation, banking, communications and the media, could in the future be the target of cyber attacks by a strategic opponent. The defense and security of these networks is in the national and public interest. A country's national security and economic well-being are at stake.

NATO as an organization can do much to establish and enhance a common cyber defense among its members. Yet it is largely up to each nation to protect its own respective networks and infrastructure from cyber attack. In this respect, each of our countries is very much in the same boat. To a greater or lesser extent we each face similar challenges in protecting nationally vital information infrastructure.

1. A Simple Conceptual Framework

At the highest levels of national government, two of the most important decisions to get right are properly prioritizing among competing missions, and balancing between short-term and long-term objectives. This is true in monetary policy. It is true in energy and environmental policy. It is vital to military success. And it is no less vital to national cybersecurity efforts.

Dr. Paul Bracken, a professor at Yale University, once wrote of the need to "model simple, and think complex."[2] Simple models help us to think about the complexity of what they reveal. A simple model[1] the author has found useful for thinking about and communicating the need to balance between competing national cybersecurity priorities is the cyber risk continuum in Figure 1 below[2].

The graphic depicts a range of cyber threats, increasing in both potential consequence and risk from right to left[3]. In this case, consequence can be thought of as the potential for harm to a nation's security or economic well-being. These threats are not unique to the U.S. but rather are faced to some extent by any information-based society. The graphic conveys that the threats of highest consequence, and their associated risks, are also likely to occur with the least frequency.

---

1 The term "model" is used to convey that this is not a quantitatively-driven plot of data.

2 The model is not backed by a data-driven assessment of risk. It is based on anecdotal evidence.

3 This paper frequently uses the term "cyber risk", which differs from a "cyber threat". Risks are combinations of threats, vulnerabilities and consequences. A discussion of specific vulnerabilities is outside the scope of this paper, which focuses on two of the three factors in determining overall risk – namely "threats" and levels of "consequence". The paper assumes vulnerabilities exist, and that threat actors differ in their capability and motivation to exploit these vulnerabilities in ways that might harm a country's economic or national security.

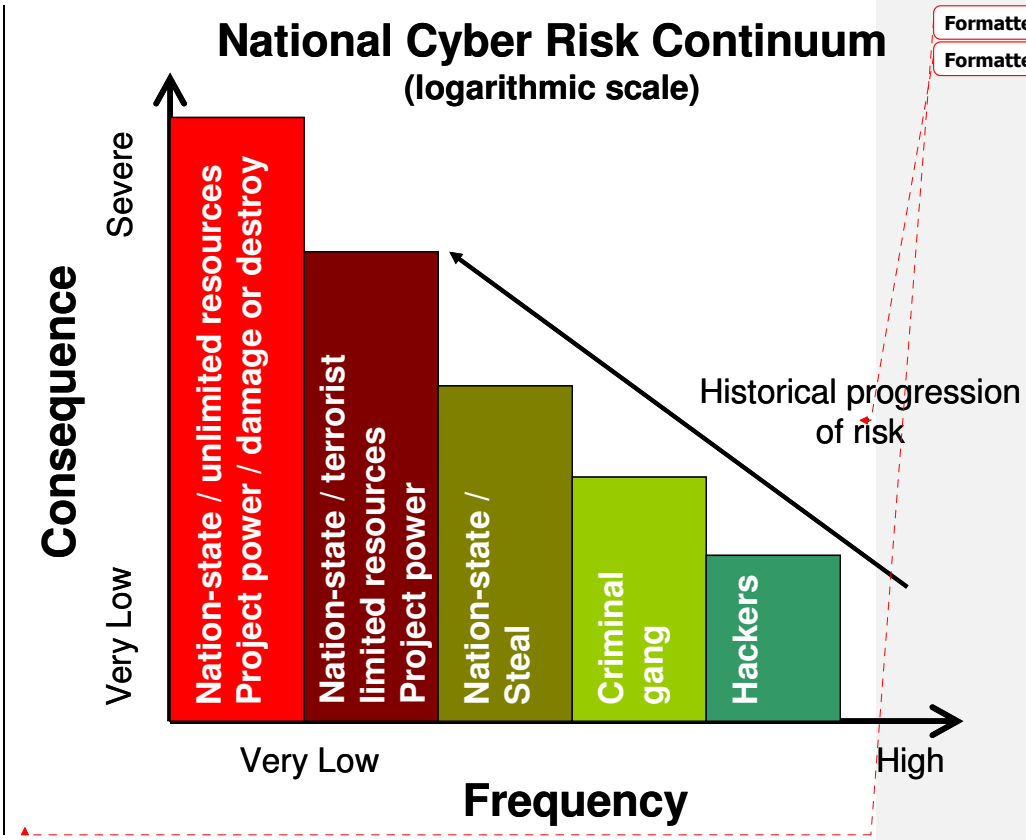

Figure 1.

On the far right of the continuum are nuisance threats including "script-kiddies" and hackers. Next in increasing consequence is cyber crime. Criminals, of course, are motivated to make money and are willing to break national and international law to do so. Cyber criminal gangs are increasingly sophisticated and the economic cost

of their illegal activity – most notably in the banking and finance sector – has greatly increased over the last five years.

Nation-states that are capable of and motivated to steal intellectual property or state secrets (espionage) pose the next threat on the chart. This is due largely to the potential resources, sophistication, and motivation they apply to achieve their objectives.

The next most consequential threat on this continuum is that posed by either nation-states or non-state actors, including terrorist organizations, which might be motivated to project power through cyber attacks on critical infrastructure. This category includes threat actors who have limited resources, time, and access to accomplish their objectives.

The most consequential threat is attack by one or more nation-states intent on projecting power, and who are willing to damage or destroy critical information infrastructure by cyber means in order to achieve this objective. Threat actors falling into this category have the necessary time, resources, sophistication, and access to do so. This category certainly includes cyber warfare.

It is important for national decision-makers to understand that cyber warfare exists on a continuum of risk. It is not going too far out on a limb to say that risks have tended to increase over time. Effective mitigation of lesser threats does not necessarily mean that more consequential threats, including cyber war, are also mitigated. It is obvious, but should be stated nonetheless, that a nation's tolerance for cyber risk relates directly to its economic and security dependence on information infrastructure.

2. Limitations of the Model

It has been wisely said that "all models are wrong, but some are useful."[3] In that spirit, the author acknowledges that the continuum is overly simplified. It shows only a few threat categories from among many combinations of threat actors and capabilities. It treats these as distinct from one another, whereas in reality nation-states, terrorist organizations, hackers, and cyber criminals might use one another, perhaps unwittingly, to achieve their respective objectives. And of course it is often impossible to tell one threat actor from another in cyberspace, given the inherent difficulty of attributing attacks to their ultimate source. Still it is useful as a construct for thinking about the problem, and for conveying some of its strategic implications to senior decision-makers.

First, it conveys the simple progression of the cyber threat – a key component of risk. Early on in the development of cyber infrastructure, we were only exposed to risk from script kiddies and hackers. As more businesses connected to the Internet, sophisticated criminal gangs emerged. Within the last few years nation states are reported to have stolen massive amounts of data from defended networks. In other words, the progression of risk has steadily moved to the left. The author believes the underlying reason for this is economic. At each step the benefits of cyber attacks to those who conduct them have outweighed the costs they incur.

This was acceptable when the potential consequences were low. But they are increasing. The current state of affairs is clearly unacceptable. In the U.S. it has been called a national security crisis.[4] Today, nation-states are beginning to understand in concrete terms the potential benefits and costs of cyber attacks used as a means of projecting national power. It may not take a great deal of a nation's cyber resources, planning time, or technical access to achieve limited national objectives.

As every businessman knows, past performance is not necessarily an indication of future activity. One cannot predict that just because the progression of risk has moved steadily and swiftly up the continuum, it will continue to do so. But an obvious question for national policy makers is this: "What set of factors might stop this progression?" A corollary question: "Should we assume the progression will continue unless the economics of the problem changes – unless costs to potential attackers can be introduced to clearly change their cost/benefit calculation?"

One way to change, or at least slow, the vector of risk is to raise the cost of attack by enabling a better defense. In the U.S., cyber defense of critical infrastructures is largely a homeland security mission. It may be that defense always lags the most potent

offense. But the goal is an *effective* defense, not a perfect one. The exact nature of that defense will vary from country to country, sector to sector, network to network, and threat to threat. It will depend on strategic objectives, an assessment of strengths and weaknesses, available resources, national capacity for research and development, and tolerance for risk, among other factors. To be effective, a national cyber defensive capability, commensurate to the level of risk, should exist before a country experiences the high consequence threat on the left hand side of this continuum.

3. An Apt Metaphor

Several years ago a United States Senator, The Honorable Robert F. Bennett, gave a keynote speech at a conference on cyber conflict. He used a sports metaphor to convey a key point. Referring to Wayne Gretzky the famous hockey player, Senator Bennett alluded to the fact that Gretzky had such a sense for the flow of the game, he could anticipate ahead of other players where the puck would be – and he skated to that position on the ice. He arrived before the puck, and was then in position to help the team score.

The author believes the Senator's point was this: an information-based society like the U.S. cannot protect its information infrastructure from the worst cyber risks unless it makes a concentrated effort to get ahead of the threat. This point is vitally important. Yes, our countries must address the threats we face today; we cannot neglect them. But for some countries it could take years, perhaps decades, to build an effective defense against the most consequential risks on the continuum. It is one thing to protect government networks. It is entirely another to protect non-government networks against nation-state cyber threats. Building a national capacity to do so will not happen overnight. And that raises another vital question for any national policy maker: "How long do we have before the most consequential threats might materialize?" Whatever a country believes that timeframe to be, if it has no effective defense in place before then, it assumes a very great risk indeed.

4. A Policy Imperative

The cyber threat never stops. Our respective operational echelons and cyber defenders have no time to come down from the ramparts. Their typical day is filled with efforts to mitigate current and near-horizon threats. But over-the-horizon risks will not disappear. Operational cadres may not have the time or present capability to deal with them, but these risks deserve more than a fleeting glance when operations allow. A country whose tolerance for cyber risk is low should devote the resources necessary to understand the most consequential threats and address the risks they pose.

Nobel Prize-winning economist Herbert Simon once said, "Short term thinking drives out long term strategy, every time."[2] This insight is the economic corollary to the Gretzky metaphor. It certainly rings true in the field of cybersecurity.

The national cyber risks faced by an information-based society are great. They may seem far in the future; but the most consequential risks must be mitigated today with action that is direct and decisive, not oblique or incremental, regardless of their frequency. Proactive steps to mitigate over-the-horizon risks will be much less costly to commerce and national security than allowing these threats to materialize. Recent

experience in other policy domains, including finance and hurricane preparedness, has proven this point.

To get ahead of the most serious national cybersecurity risks, including that of cyber warfare, a country's cybersecurity leadership must seek an appropriate balance of resources, energy, and focus between those threats that are most frequent and those that are most consequential. Creating the conditions in government where infrequent threats can be understood and addressed is easier said than done.

In each of our countries, the organizations that have defensive cybersecurity responsibilities perform one or more of three different missions. They fight cyber crime. They defend government networks, including those that are used by civilian agencies, the military, and the intelligence community. And in some cases they must help protect non-government networks that qualify as critical national infrastructure. As we all know, these are mostly owned and operated by the private sector. They include the data, hardware, software, and control systems that undergird our financial markets, the generation and distribution of electricity, modes of mass transportation, and our vital telecommunications. They support thousands or millions of competitive business models - each one unique; and they are operated mostly with economics in mind.

This last mission raises two additional policy questions for many of us. The first is this: "Against which cyber threats on the continuum should our governments be held responsible for protecting the private sector?" At every point on the continuum, commerce is vital. So are civil liberties. Clearly, the bias at the lower end of the risk spectrum should be weighted toward private enterprises taking the lead for managing these risks as they relate to individual business models. Equally clearly, no private enterprise – no matter how well capitalized – can bear the cost of defending itself against destructive nation-state attacks. In this case the opposite ends of this continuum are a bit like the opposite poles of a political spectrum; it is fairly easy to see what exists at either end, but it is much harder to characterize the middle.

5. Drawing the Line between Security and Defense

This leads to the second question: Where on this continuum should a country's leadership draw the line between security and defense? Where does one stop and the other start? A country cannot debate this question forever. Leaving it unanswered leads to a situation in which no one – not the defense community, not the security community, nor the private sector, is clear about responsibilities. Lack of mission clarity leads to lack of authority, resources, and capabilities. And that comes at the expense of neglecting the high end of the consequence spectrum.

Figure 2 depicts one way of thinking about the difference between cyber "security" and cyber "defense" – at least for a western democracy such as the U.S. It shows two parallel lines - both of which are drawn rather subjectively[4]. The area below the grey

[4] Exactly where the security and defense boundaries should be drawn in relation to the continuum of threats is worth careful policy debate and consideration. In this case they are drawn for illustrative and discussion purposes only; in reality they could be higher or lower. Moreover, it may well be that the higher end of the "security" boundary is not static across all threats, but rather it increases in stair-step fashion as the threat increases. By this is meant that the private sector might be enabled to participate at higher and higher levels of capability in their own (and the national) defense as threats and risks escalate.

line is labeled “security”. In this case, the term “security” indicates that the clear bias should be toward expecting private enterprises to bear primary responsibility for managing risks in this range. Naturally they would do this primarily out of fiduciary responsibility to their stockholders – but also in some cases as part of a regulatory framework.

This does not mean that the private sector should be *solely* responsible for mitigating risks associated with threats at the lower end of the spectrum. Cyber crime, for example, is an area where the private sector must work with law enforcement to address the threat adequately. Many national Computer Emergency Readiness Teams (CERTS) also provide incident services to the private sector that help them mitigate risks even from the lower tier of cybersecurity threats.

It does mean, however, that both government and industry should agree that the primary metric through which the risks associated with these threats are cooperatively managed is that of maintaining competitive business models. Mitigation efforts must sustain profitability for individual businesses, value chains, and complete sectors of business activity.

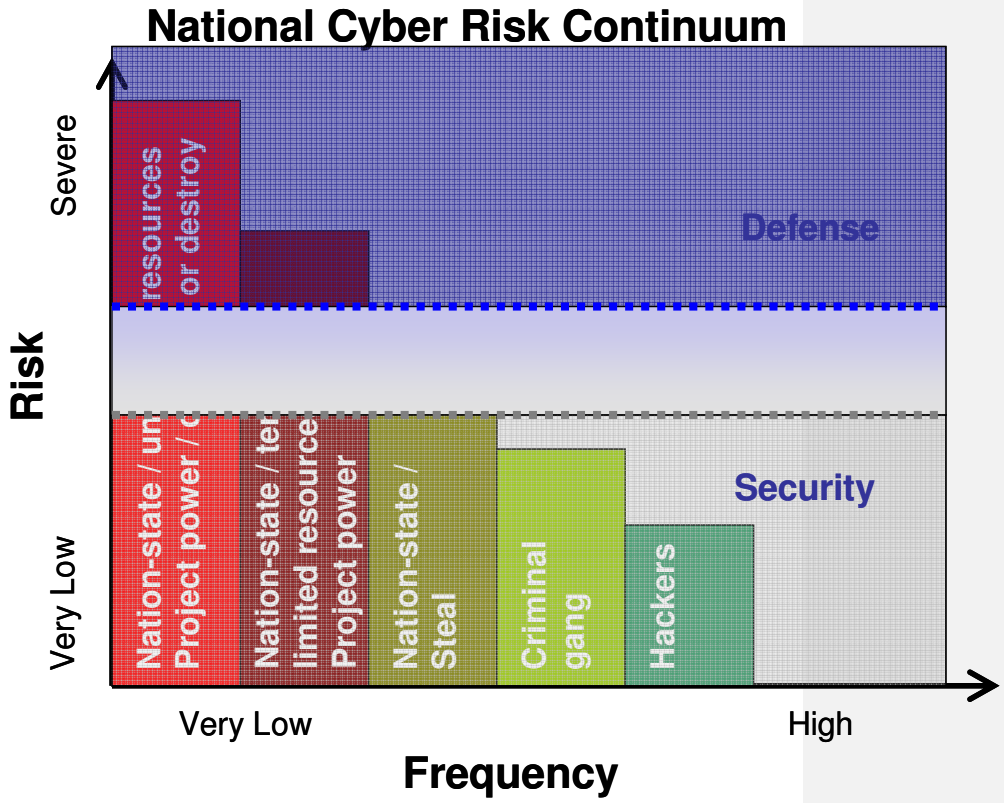

Figure 2.

Note that on this graphic the "security" domain extends across the entire spectrum from left to right. One important conclusion is that private enterprises – at least those that operate critical infrastructure - must have some responsibility, presumably backed by demonstrated capability – to assist in mitigating all categories of cyber threat - even those that contribute to the most consequential national cyber risks.

The extent of that responsibility is a question of strategy. At its most basic, the central question is this: should privately-owned critical information infrastructure be defended against the most consequential threats from "within the enterprise" – meaning by experts who operate and know the importance of each byte on those networks on a daily basis? Or should they be defended by government cybersecurity experts, using nationally developed capabilities from outside the normal perimeters of most business networks? Both have advantages. Both also present very difficult challenges. A balanced strategy might include both, but the question then becomes: what is the appropriate balance between the two? Answering this question is fundamental to national cybersecurity efforts.

The area above the blue line is labeled "defense". In this case the term conveys that risks resulting from these threats are systemic and could be nationally debilitating. Government should be primarily accountable for addressing this tier of threat, even though operational responsibilities must inevitably be shared between government and the private sector. Indeed, the threats at this end of the spectrum are so potentially severe that their mitigation should be thought of as a *mission to be performed* rather than as *something to be managed.*

These threats are simply beyond the scope of private sector capability to adequately address. Both government and industry should agree that the primary lens through which these high-tier threats are addressed is one of national security. If national security is at risk, commerce is also at risk. There should be no question about priority in this domain. National security must take priority over commercial interests for those who are assigned responsibility to manage the highest consequence threats, whether that assignment is given to the defense community or the homeland security enterprise.

6. The Sticky Middle Ground

In between is a shaded area in which the delineation between security and defense is blurred. It is in this area where roles and responsibilities between government and industry are most difficult to define. Addressing threats that fall into this domain offer the most difficult decisions. This is true for two reasons.

First is the strong potential for conflicts of perspective and for competing interests. The private sector must compete; fiduciary responsibilities require businesses to maintain their focus on the bottom line. In most cases, their risk horizons are invariably short. On the other hand government must support and enable commerce, but not at the expense of providing for the common defense – a constitutional requirement in the U.S. It must take necessary steps to manage long-term risks. Inevitably, tension exists between these differing perspectives and responsibilities.

Second is the extent to which mitigation decisions for risks in this middle tier involve unknowns. The complexity of cyberspace; its tendency to create unforeseen interdependencies; the way it immediately transmits and links impacts of decisions made remotely across great distances and geographic, political, and organizational

boundaries; the potential for small, hidden vulnerabilities to result in highly leveraged consequences; and its newness as a domain for conflict, all greatly increase the fog of risk management and crisis decision-making. This is especially true in the domain of risks that occupy the middle of the consequence spectrum.

This leads to another important insight. It is incredibly easy to get bogged down in mitigating mid-tier risks. Recall that the progression of threat – and by extension the progression of risk- reached this middle tier by starting at the bottom end of the consequence spectrum. The historical bias in dealing with cyber risk has been to look at it through the lens of commerce, not national security – and to reinforce the emphasis on short-term thinking rather than long-term strategy.

These factors, together with the tendency for conflicting perspectives and difficult decision-making against this middle tier of threats, *create an operational environment in which the struggle to devote any meaningful time and effort toward getting ahead of the most consequential threats is a real challenge.*

One way to meet this challenge is simply to emphasize efforts that mitigate the most consequential risks. A nation's cyber leadership could decide, for example, that it should apply significant early resources to the left end of the continuum – to mitigating the national security risk associated with defending critical infrastructure against nation-state threats. Over time it could capitalize on these resources by applying them against lesser risks. In this way it could ensure that it does not grind to an operational halt short of accomplishing its highest strategic priorities. It also could gain the most value from its resources.

Other ways to emphasize the most consequential threats and risks: (1) develop a long-term war-gaming practice that continually refines the policy, legal, economic, operational, and technical issues associated with the high end of the continuum; (2) ensure planning scenarios for exercises and war-games focus on these threats; and (3) require that national and sector risk assessments cover the entire risk continuum.

A logical step for any country's cyber leadership is to undertake a continual effort to assess risk across this spectrum. Part of this effort should include identifying the subset of discrete vulnerabilities in critical information infrastructure, which if exploited would have the most debilitating consequences to national or economic security. Developing an appropriate strategy for mitigating each of these discrete risks should be a joint effort between government and the private sector. But government owns the responsibility, and should have the authority, to say when or whether the most severe risks have been acceptably mitigated.

7. Capability v. Mission

Of course, delineating risk responsibilities between government and the private sector is only part of the solution. In large bureaucracies such as in the U.S. the imperative to clearly define defense from security exists for another reason, and that is the need to clarify missions between government agencies, and assure each mission is supported by adequate capability.

If one's mission responsibilities are unclear, it is impossible for one to know if his capabilities are sufficient.

Figure 3 shows the threat continuum overlaid against an assessment of capability vs. mission. It supposes the existence of an organization with a given risk mitigation capability. If this organization is assigned a mission of defending critical information

infrastructure against criminal threats and theft of intellectual property, Mission (A), then its capability is sufficient. If however, its mission includes defending the same infrastructure against destructive cyber attacks at the high end of the consequence spectrum, Mission (B), then its capability is woefully inadequate and leaves unmitigated risks.

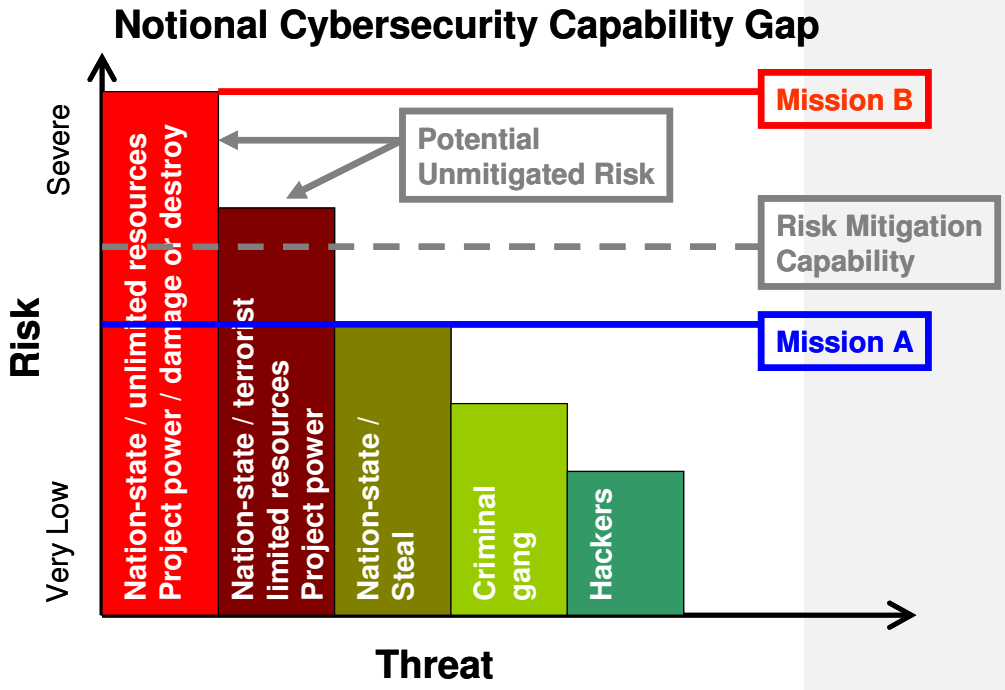

Figure 3

By inference, it is vitally important for national leadership to understand which threats on the continuum it is most interested in addressing, and receive a straightforward assessment of national capabilities mapped against those threats. This is true for individual government organizations as well. Any delta between mission and capability deserves the focus of decision-makers.

8. Summary

For which discrete categories of threat on the continuum are the defense community, the security community, and the private sector ultimately responsible? Policy leadership in any country must make that clear. Only then can operational leadership ensure that short-term actions and operational objectives measure up against appropriate long-term strategy.

References

[1] "Defending Against Cyber Attacks". 2009. North Atlantic Treaty Organization. 9 July 2009 http://www.nato.int/cps/en/SID-D30474D0-A97D6B01/natolive/topics_49193.htm

[2] Bracken, Paul. "Net Assessment: A Practical Guide," *Parameters* (Spring 2006), p. 100. http://www.carlisle.army.mil/usawc/parameters/06spring/bracken.pdf

[3] Box, George E. P.; Norman R. Draper (1987). "Empirical Model-Building and Response Surfaces". Wiley, p. 424. ISBN 0471810339. Wikiquote. 9 July 2009 http://en.wikiquote.org/wiki/George_E._P._Box

[4] Gross, Grant. "U.S.Government Focuses on Securing Backdoors in Tech Product". *Security Central* (September 2008). Infoworld. 9 July 2009 http://www.infoworld.com/d/security-central/us-government-focuses-securing-backdoors-in-tech-products-853