Tactics and Technicalities Undermining Strategy:

Cyber Security is Distracting National Security Communities

Brigadier Martin White

ABSTRACT

National security communities cannot protect all their information. Yet the exigencies of cyber security and identified network vulnerabilities are trumping more strategic consideration of information protection, and national security communities have found it difficult to adhere to clear and defensible information protection principles. A more strategic approach would focus on identifying and prioritizing the most important organizational information; a defense that aligns information security resources to the most important information, with a clear view of the actions needed to protect against the intelligence capabilities of strategic competitors; and, established mechanisms for situations when preventive security measures will so often fall short, which include standing deception plans and well-coordinated reparative measures. Without defensible principles, the immense cyber security investments being made will not have the desired information security effect.

INTRODUCTION

Should national security communities[1] care as much as they seem to about cyber security?[2] The orthodoxy would suggest that this is an absurd question. National governments have habitually accelerated the provision of resources to improve cyber security.[3] Strategic and technical commentary alike define the cyber domain as a central consideration in any notion of success in future conflict.[4] Credible commentators are not questioning cyber security's importance to national security or arguing to limit cyber security resources. More cyber security is the convention. Accordingly, national security communities have made considerable effort to broadly improve cyber security.

Brigadier Martin White is an Australian military officer. He has served in a range of military appointments, including operational service in Timor Leste, Afghanistan, and Iraq. Martin received a Conspicuous Service Cross in 2016, among other awards. He completed his Ph.D. in defence policy and energy security from La Trobe University. The views represented in this article are the author's alone.

Nonetheless, the familiar aphorism "tactics without strategy is the noise before defeat" comes to mind. Traditional national security models that demand high levels of broad information assurance—including of classified information—are becoming increasingly untenable as information becomes easier to disclose. Although it is not specific to a particular national security community or country, a preoccupation with cyber security is analogous (in the contemporary security environment) to a pre-occupation with the tactical and technical aspects of security. This preoccupation has precluded a more strategic concept of protecting the most important information and information links[5]—a nation's Crown Jewels—based on clear and defensible principles. Attention to cyber security is crowding out the more important considerations of how to protect a nation's most important information in the face of an immense contemporary intelligence threat. A strategic approach irrefutably requires extensive cyber security efforts; cyber security is a fundamental technical and tactical tool that is essential for the defense of critical information, but it is not the only tool that is needed. National security communities should look beyond this single aspect, if major investments in cyber security measures are to prove meaningful.

The rapidly changing threat environment has made it difficult for policymakers to enunciate clear and defensible information protection principles. The dearth (in the cyber security literature) of concepts such as: information protection beyond cyber security; senior leaders as the most valuable intelligence targets; the value of deception in defending information during peacetime;[6] the profound vulnerability of classified information to compromise; and the importance of reparative actions as a key and integrated component of national strategies suggests that national security communities are encumbered by the need to address urgent cyber security challenges at the expense of more strategic consideration of information protection.

There are six principles that may contribute to the overall coherence of a national security community's approach to protecting its Crown Jewels. These principles outline the need to clearly identify the most important information; to ensure detailed understanding of all intelligence capabilities used by strategic competitors; and to establish mechanisms to deal with the failure of preventive security measures. The principles are:

1. Cyber security represents a critical tactical and technical tool but should always be framed within a broader strategic concept to protect a nation's Crown Jewels.
2. National security communities must clearly prioritize the information they seek to protect. But even if information protection is done well, a national security community will still only be able to defend a fraction of its information over time.
3. The intelligence capabilities of strategic competitors should be habitually assessed against the protections offered to a nation's Crown Jewels.
4. Senior leaders should be the highest priority for information protection measures.
5. Planned deception measures should be enacted as a standing operation in peacetime, to provide a temporal advantage in the event of a conflict.
6. Reparative arrangements in the aftermath of information compromise should be more comprehensively integrated in national strategies.

Senior leaders should devote less attention to the tactical and technical aspects of cyber security and base their guidance on defining and defending the most important national information using these six principles, where such protection will offer a decisive advantage in the event of conflict.

THINKING LIKE A SPY

1. Cyber security represents a critical tactical and technical tool but should always be framed within a broader strategical concept to protect a nation's Crown Jewels.

Over recent years, national security communities have sought to consolidate their vast numbers of disparate information and computer networks,[7] and to provide greater information security to the military industry.[8] In Australia, the Department of Defence has minimized the number of standalone information systems in operation.[9] More than 700 standalone systems, regularly built by military units who needed to achieve a specific task, were sometimes not maintained with sufficient cyber security hygiene and presented a risk to organizational information.[10] The Department of Defence pursued the closure of these standalone systems as a priority. Progress reports identified the number of standalone systems taken offline as a key metric.

Once the vulnerability was recognized, the efforts to shut down an individual system as soon as possible could be considered quite rational—a systematic solution (a reduction in

attack surface, to allow cyber security resources to be more focused) to progressively address a challenging, identified risk. However, when looking at this solution from an intelligence targeting perspective, another view emerges.

If an intelligence collector had identified the Australian military's standalone systems as priority targets, that collector could observe the system closure process. It is reasonable for the intelligence collector to assess that the systems first closed were the easiest to remove from operation. In a process that prioritizes withdrawing individual systems as soon as possible, the first closed systems may well contain the least important organizational information. If the closure of a specific system would negatively impact an important organizational function, that higher priority system would need to remain operational for longer. This simplifies targeting for the strategic competitor, leaving them to take actions such as metadata analysis or exploitation of known software vulnerabilities in order to obtain intelligence. And higher value information was raised in profile because a technical and tactical approach was applied. The standalone systems needed to be closed because of intelligence concerns, yet the likely actions of an intelligence collector were inadequately mitigated.

The simplified risks presented in this short case study are by no means unique to military organizations or to any specific country. Most countries are grappling with the same challenges, often under intense public or political scrutiny. In the rush to enhance cyber security in an immediate and tactical way through decisive actions, it is possible that the actions taken are unintentionally weakening security associated with the most important national information, and do not clearly account for how intelligence collectors operate.

Cyber security is a term used so commonly now that it is often not clear what it encompasses or what it is that national security communities must secure. The 2018 US Department of Defense Cyber Strategy was non-specific, identifying the need to "defend its own networks, systems (and) those networks and systems operated by non-DoD Defense Critical Infrastructure"; that is, virtually everything that might be related to cyber.[11] The term is regularly used with impossibly high criteria,[12] and with non-specific objectives relating to whole-of-organization (or even whole-of-nation) cyber security. National cyber strategies all have excellent intentions, but they consistently try to satisfy many competing priorities, with little sense of what bounds the problem and focuses the resources.[13] And the demand for more cyber resources is relentless.[14]

Of course, definitions and boundaries matter little to intelligence collectors, and they have few concerns about where they get their information.[15] To be sure, cyber operations are very effective because so much information is now digitized. But whether information comes from a cyber-exploitation operation, electro-optical satellite imaging, mobile telephony interception, or human intelligence, is largely irrelevant. In fact, many nations deliberately seek to gain intelligence from a broad range of sources to increase confidence in their assessments. Therefore, actions to pursue cyber security in a manner that is disengaged from the broader

problem of information protection would be futile, if other means of obtaining the same information are also available for an intelligence collector.

Further, an intelligence collector would be attentive if their national security target sought to broadly apply cyber security measures across many networks and systems—to seek an average standard of protection for everything—rather than focus security measures on their Crown Jewels. An effort to apply similar levels of information security across many systems may have had some merit prior to the information age, where any intelligence collection was felt to have some value. However, as information has become far more accessible, the greatest intelligence value can be gained by focusing the collection of multiple intelligence assets on the highest value information.

If a national security community is not clear and consistent over time about what its most important information is; has not anticipated seeing much of its classified information compromised over time; and has not protected its most important information in a prioritized way, a concentrated intelligence effort could prove particularly damaging.

Put simply, intelligence collectors will consistently seek the most valuable information for the least effort and will often aggregate a diverse range of collection capabilities to obtain important information. When considering the problem from this perspective, averaging out cyber security resources across many information systems may not be most effective and may even be futile if the highest priority information disclosures can occur through non-cyber collection.

A FAIR GO FOR ALL (INFORMATION)

2. National security communities must clearly prioritize the information they seek to protect. But even if information protection is done well, a national security community will still only be able to defend a fraction of its information over time.

Priorities are inherent in all national security decisions. Senior leaders must constantly make choices that privilege certain missions, agencies or capabilities above others. It is therefore surprising how rarely the idea of information prioritization features in policy and commentary, when commentary on cyber security is so prolific and when information is considered such a strategic resource. Aspects of prioritization sometimes appear, as in the periodic debate about the importance of protecting (or not protecting) metadata. But this is the exception.

Information needs to be prioritized to allow the most important information to be defended. This tenet is not consistently represented in national policies or in cyber commentary. Conversely, equity is often the governing aspect. There is a sense in policy and commentary that all information can be protected or, that national security communities should try to offer near-complete protection. An apparent failure to protect information—even if not of

particularly high value—from cyber exploitation is often met with heavy criticism. However, trying to protect all information (including classified information) and mitigate all possible vulnerabilities—either as a deliberate policy or through the inertia of continuing what is already established—will remain prohibitively expensive[16] and will divert resources from the most important areas.

To be sure, official information necessitates a range of technical security measures that demonstrate its priority over information held in the private sector. For example, information classification, the vetting of personnel and physical security measures are long-established methods that demonstrate prioritization of higher-value information is necessary and is important to national security communities. Yet national policies relating to cyber security contain few references to the prioritization of information to defend, and rarely acknowledge that cyber-attack is but one of many vectors that a strategic competitor may use to obtain or disrupt information.

Two recent authoritative national policy documents underscore this point. Neither the 2018 US National Cyber Strategy[17] nor the 2016 Australian Cyber Security Strategy[18] prioritized the most important information as a key aspect of the strategy, nor did either strategy enunciate that cyber-attacks are only one way for a threat to gain information or disable a system. National strategies consistently highlight the growing resources being applied to cyber security[19] however, the magnitude of resourcing is a poor gauge if the protection is not optimized. For instance, Australian national cyber security resources have historically been allocated to respond to "the full range of cyber incidents from national crises to...individual members of the public,"[20] indicating that information is treated equally. This is not consistent with a national policy that prioritizes resources to contend with the most significant threats.

There are often minor references to information prioritization in lower-level technical documentation. For example, the Federal Communications Commission's cybersecurity advice to small business refers to the protection of "critical data."[21] A 2019 Australian Information Security Manual articulated a sub-principle that "the identity and value of systems, applications and information (should be) determined and documented."[22] Such references demonstrate that the concept of information prioritization has been enunciated, but these scant references do not represent a fundamental approach to information security.

Commentators have mostly approached cyber security in a similar way, seeking urgent, broad improvement but with few references to prioritization. Some commentators have argued that certain industries should be prioritized,[23] although national governments are sometimes ambiguous when describing the parts of the economy that constitute critical industries (or perhaps more importantly: what industries are less critical).

A common cyber security metric has been the number of cyber security specialists in employment, with the consistent view that there are too few and they do not have sufficient

training.[24] The recruitment of cyber specialists for national security purposes is clearly an important challenge, and most security communities believe their nation needs more.[25] This may well be so. But such discussion must be contingent on the information that must be protected. The necessary size of a cyber workforce will be difficult to quantify until there is a clearer understanding of information protection priorities. Where there are other non-cyber, intelligence vectors where certain information can be compromised, the size of the cyber workforce is only part of a solution. And public debate rarely touches on the need for a workforce to be assigned to other information protection functions, such as mitigation against a strategic competitor's satellite collection; Russian military forces occupying Ukraine may wish they had considered this type of intelligence collection in greater depth.[26]

There are rational explanations for the lack of attention to information prioritization. First, there is a genuine public and political desire for national security information to be more secure, and policymakers do not want cyber-attacks against their national security community to succeed. As a result, some commentators view data loss as a preventable failure.[27] Second, policymakers want to be seen to be listening to and responding to the concerns of all citizens, and many citizens are indeed concerned about cyber security.[28] Stated priorities for information protection could ostracize some parts of the public or the security community. Third, the cyber threat is so immense that it can be difficult to establish a principles-based strategy, as "the urgent" overrides "the most important" and there is a need to be seen responding to all cyber vulnerabilities. Fourth, there is a high level of trust in classified networks because of the additional security measures established within these networks, and this could cause complacency. Finally, there is a degree of faddism relating to the (relatively novel) topic of cyber. Some commentators may profess views while having limited knowledge of the subject. It is also possible that no policymaker wants to be seen to accept a perceived or relative weakening of cyber security, which would occur if some areas were preferred over others.

Ultimately, a lack of prioritization and the belief that any information compromise is bad detracts from the pursuit of a more strategic approach to information protection. A strategic approach would coordinate prioritization of cyber and non-cyber efforts to achieve a credible information defense for a nation's Crown Jewels. This means that other information becomes a lower priority and may be more readily disclosed. National security communities clearly have information and information links that are critical to their business. Whether these information and information links are plans for new military hardware, or specific secure links between intelligence agencies, or a specific highly sensitive mission, national security communities should clearly understand where resources must be applied to optimize information protection.

When nations make immense cyber security investments, they strongly signal that information security is a priority. But if information security truly is a priority, national security communities must focus beyond tactics and technical aspects. They must prioritize the

information that must be protected to maintain an advantage in the event of a conflict, then seek to protect these Crown Jewels (through cyber security and through other non-cyber investments in security) against strategic competitors. In this way, nations will consider the intelligence capabilities available to sophisticated strategic competitors.

THE WHOLE TRUTH

3. The intelligence capabilities of strategic competitors should be habitually assessed against the protections offered to a nation's Crown Jewels.

The intelligence threat from strategic competitors is largely a concealed problem. Senior leaders often do not know if intelligence collection against a national security community has been conducted, and the public will know even less. Counterintelligence can also be an expensive and practically limitless undertaking.[29] With so many competing priorities for resources and for senior leaders' attention, few are enthused by the prospect of a largely amorphous and distant problem with challenging metrics and an expensive upkeep usurping what is currently seen as a relatively straightforward (and mostly unquestioned) ability to assign resources to cyber security.

Put simply, why would national security communities make information protection a bigger problem? The answer to this question lies in the intelligence threat that national security communities face from the full range of intelligence collection capabilities maintained by sophisticated strategic competitors. Perhaps most critically, intelligence collection during peacetime has the potential to decisively jeopardize a nation's preferred operating model in the event of conflict.

Most nations need no convincing that their information is targeted by strategic competitors. However, the extent of intelligence collection is rarely fully explained, and the prominence of cyber threats masks a complete view of threats to critical information. Intelligence collection now comprises an immense range of sophisticated capabilities. These include satellite and ground systems;[30] many human intelligence techniques;[31] underwater acoustic collection systems;[32] video surveillance;[33] and, un-crewed intelligence collection platforms,[34] to name just a few.

Underpinning intelligence collection is a range of fusion and analysis capabilities, now enabled by technological advancement in data analytics. Sophisticated fusion and analysis capabilities offer a range of benefits, such as allowing intelligence to be focused against targets of interest and ensuring that data can be quickly aggregated. China's prioritization of "informatized warfare" and of its military Strategic Support Force are examples of national-level efforts to improve information fusion.[35]

The following diagram outlines many of the intelligence collection capabilities that are currently targeting national security communities. Each of these capabilities represents a discrete means to disclose information. And when aggregated against a specific information requirement, it is difficult for a national security community to mitigate, especially over time.

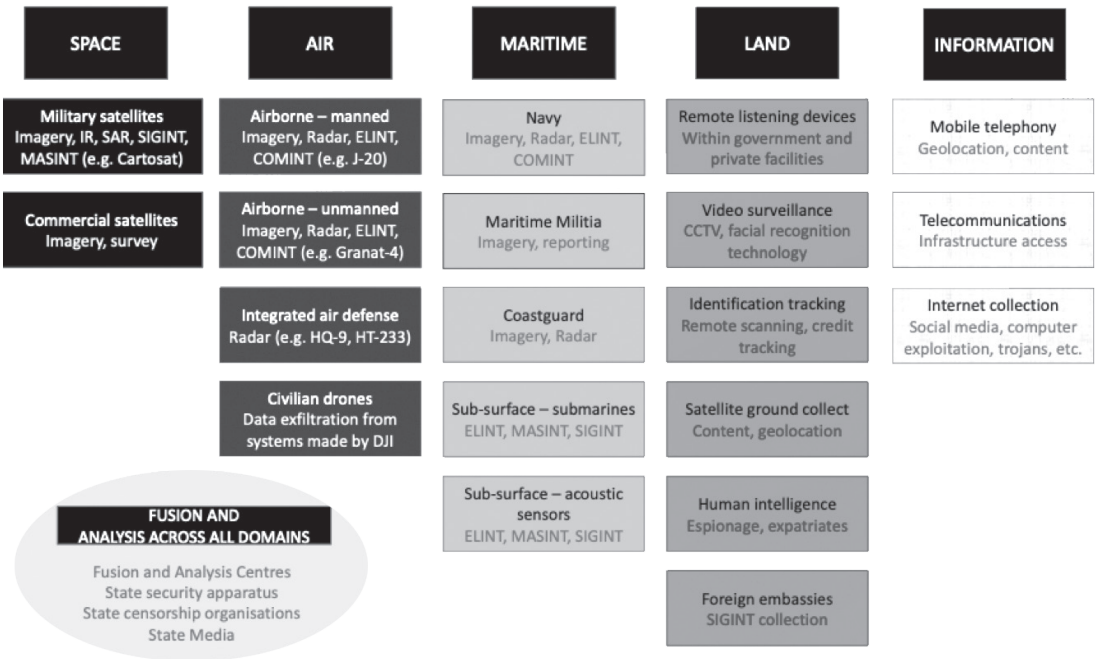

Figure 1: Intelligence collection, by domain

To be sure, every strategic competitor has competing priorities that demand intelligence effort. However, intelligence resources will mostly be concentrated against valuable information targets; particularly national security community targets. If a national security community does not identify and offer adequate and consistent protection against a range of intelligence threats over time, it is foreseeable that the most important information will be compromised at some point or another.

If a national security community does identify its Crown Jewels and seeks to deny access to this information to sophisticated strategic competitors, the information would need to be protected, over time, from all forms of threat intelligence as noted in Figure 1 and not just from cyber exploitation. This is no trivial undertaking. Figure 1 suggests that a strong cyber security capability would only partially protect a national security community's Crown Jewels. Cyber security alone does not mitigate the intelligence threat. Indeed, a nation with strong cyber security but weak security (or unclear security objectives) in other domains invites information theft by herding intelligence collection into its weaker domains. Typically,

sophisticated intelligence assessment organizations seek information that has been derived from a range of sources to provide greater validity to their assessments.

Alternatively, nations are not compelled to benchmark against the most sophisticated intelligence threats. There are different levels of information security that a national security community may achieve, and it may be reasonable for senior leaders to pragmatically accept more risk while ensuring information protection against a less sophisticated intelligence threat. For example, senior leaders may accept that sophisticated threat intelligence will gain more information than they would prefer, but establish measures to ensure that terrorist groups are unable to access the personal details of intelligence personnel. Senior leaders regularly make these sorts of risk management decisions across all parts of national security strategies.

But most nations and their security communities have not made this trade-off. Given the considerable investments made by nations in cyber security in recent years, and the strident policy statements outlining the need to mitigate cyber-attacks,[36] one can only conclude that nations have the intention to protect important information from the most challenging intelligence threats. As stated, focus on cyber security does not offer this protection. It makes little sense to invest significantly in cyber security without dealing with the threat to the same information from all types of intelligence collection, or without specifically prioritising protecting the most important information. The broader aspects of information protection (beyond cyber security) are largely absent from the public discourse.

Figure 1 also shows information trends that national security communities must consider. First, there are few geographic and temporal boundaries for intelligence collectors. While some have sought to characterize intelligence collection purely in a conflict context,[37] most of the identified threat intelligence capabilities can be directed towards priority targets at any time. For example, military and commercial satellite collection can often occur anywhere in the satellite footprints and will mostly be conducted outside periods of conflict.

Second, Figure 1 makes no delineation between "private" and "work" communications systems, or between "training" and "operational" communications. If a senior leader uses a personal email account, those communications are considered an equally valid target as an official email account. Training activities are as valid intelligence targets as operational deployments. And a temporary lapse in protection can result in permanent information disclosure.

Third, many of the data sets from individual intelligence collection methods can now be compared to other data sets, offering a range of insight to a strategic competitor that may not even be apparent to the targeted nation. Protecting a small amount of specific information, over a long period of time, is becoming an immense challenge.

LEADERSHIP IS LESS LONELY WITH A CONSTANT COMPANION

4. Senior leaders should be the highest priority for information protection measures.

Intelligence agencies are no different from other organizations in that they seek the greatest possible effect at the lowest cost. It may be a popular mantra that a country like China will focus on a "thousand grains of sand" intelligence strategy,[38] but this surely misses the reality that threat intelligence agencies will seek the most efficient way to access a nation's Crown Jewels.

While sources like insider threats will remain valuable, sophisticated intelligence collection is likely to focus on national security communities via two main vectors. First, intelligence collection will target senior leaders. Second, intelligence agencies will collect massive quantities of lower-value data, on tactical platforms, more junior personnel and communications systems, to undertake big data analysis. The first method is very efficient and may provide authoritative information; the second method will establish correlations that may not otherwise be apparent and can improve a strategic competitor's technological capacity.[39]

Senior leaders can reasonably be considered a rich source of intelligence for a strategic competitor and should anticipate foreign intelligence agencies being their perpetual but unseen attendant. This is because senior leaders handle information that is authoritative, timely, accurate, and distilled. Further, senior leaders are consistently mobile due to the nature of their work. While senior leaders will have access to equipment and training to provide information security, they also often rely on poorly secured communications systems (such as mobile telephones and the internet), effectively voiding some of the established systemic security advantages. Senior leaders also leave lengthy trails of metadata breadcrumbs through their often-extensive communications.[40]

Indeed, there is ample evidence of the problems associated with relying on specific intelligence that is not derived from senior leaders. Secretary of State Colin Powell famously based his 2002 justification for the Iraq invasion on communications intercepts of mid-level Iraqi officers.[41] Subordinate officials will consistently not have the same context or information accuracy as senior leaders. Therefore, targeting senior leaders meets the requirement for intelligence collection efficiency—importance of information, accuracy and timeliness of information, and ease of access.

There is little reference in strategic policy or cyber security literature about the fact that senior leaders make the best intelligence targets, or should be a priority for cyber security. This is a shortfall in the literature which skews the view of cyber security priorities and necessary measures to protect Crown Jewels. While some may argue that it is obvious that senior leaders are a primary target for intelligence, it is difficult to conclude that their information security is consistently prioritized.

National security communities' most important information will be handled mostly by its most senior people. The fact that senior leaders rely heavily on poorly secured communications platforms, thereby negating many of the advantages associated with specific security measures designed for senior leaders, underscores the intelligence opportunity for any strategic competitor. Contemporary cyber security policy and commentary only occasionally emphasize this point. The tactical and technical approach to cyber security has trumped a more strategic consideration of protecting a nation's Crown Jewels.

FOOLING SOME OF THE PEOPLE, SOME OF THE TIME

5. Planned deception measures should be enacted as a standing operation in peacetime, to provide a temporal advantage in the event of a conflict.

Returning to the Australian military's challenging standalone system problem (described earlier), one alternate approach follows. The objective of this alternate approach is to close the systems with higher value information as soon as possible, while using the lower value systems to distract intelligence collectors.

The Australian military will initially leave all of its standalone systems operating, to prevent easy identification of the highest value systems. Over time, some of the systems with the lowest value information will be deliberately made less secure (for example, by failing to patch software vulnerabilities), making them comparatively easier cyber targets. Additional low value or bogus information will be added to the lowest value systems, and these low value systems (and the apparent desire to close them down) will be more widely known by intelligence collectors. In the intervening period, the priority will be placed on hardening the most important standalone systems and getting the information ready to be transferred to a more secure enterprise network. The highest value systems will then be withdrawn, before the lowest value systems.

Such an approach may or may not have been feasible for the standalone system problem. However, the establishment of a credible operational deception plan during peacetime to protect a nation's Crown Jewels and provide a temporal advantage during conflict will often be viable and offer great benefit. In this example, deception measures raise the cyber risk for some lower value systems but reduce the overall enterprise risk associated with the entire standalone system problem. Deception may even turn existing information risk into an intelligence opportunity, as a national security community can monitor intrusions onto the lower value systems.

Even after prioritizing the Crown Jewels and mitigating the specific risks associated with sophisticated intelligence collection, a national security community's information can still be compromised. This is an information age reality. An operational deception plan resourced and conducted during peacetime provides an additional layer of protection to a nation's

Crown Jewels. Such an approach accepts that national security communities must be on an operational footing at all times. Some have termed such a peacetime approach as gray zone operations.[42]

Deception is well understood across national security communities. Some agencies and departments have existing doctrine to leverage. Some of this doctrine identifies the importance of deception to cause an adversary to "squander intelligence assets" and "form inaccurate impressions."[43] If national security communities accept that they cannot prevent a strategic competitor from gaining access to important information at all times, deception offers a second chance to protect or sufficiently obscure a nation's Crown Jewels.

An operational deception campaign should be centrally coordinated and have numerous aims. It may seek to: make certain capabilities appear stronger for deterrence reasons; make it difficult for an intelligence collector to distinguish real information from false information; make certain information more prominent to induce a certain action; limit exposure of certain national capabilities that would be critical during conflict; and confuse a strategic competitor as to who may be a key decision-maker in different situations. Rather than apply deception measures across all information sources, an operational deception plan should be prioritized to deceive intelligence collectors if they gain access to the security community's most important information.

Deception must be coordinated, but it does not demand perfection. In some cases, presenting multiple alternative pieces of information may reveal a deception campaign, but still prevent a strategic competitor from understanding a situation clearly. Deception can also be effective against non-cyber threats; for example, deliberately inserting bogus information onto a government information system may mitigate some of the risk associated with an insider threat (like the case of Edward Snowden) stealing information.

To be sure, deception entails some reputational and operational risks. First, in a society that values transparency and honesty, deception represents a partly conflicting approach. If a security community actor was publicly exposed injecting bogus information onto a government information network, how would this be perceived? Second, if a deception operation is exposed, a national security community may have surrendered information it did not need to give up, or a strategic competitor can view the typical deception activities. Third, if not done properly, there is a risk that the organisation could deceive itself in various ways. However, these risks can be mitigated by using deception measures sparingly and as a second chance only for the most important national security information.

In summary, even if a national security community has prioritized resources to harden its most important information, the most sophisticated information protection measures can sometimes fail. Deception offers a second chance, and the application of deception measures should be prioritized towards safeguarding the highest value information.

PLANNING TO FAIL?

6: Reparative arrangements in the aftermath of information compromise should be more comprehensively integrated in national strategies.

The need to conduct reparative actions and consequence management[44] after a significant information compromise is well known to cyber practitioners but is less prominent in national cyber security strategies. For example, Rothrock argued in the Fall 2017 *The Cyber Defense Review* that an effective plan requires security, but also requires "resilience: the ability to fight back, quickly and effectively."[45] Given the extraordinary rate of information compromises relating to governments and businesses that are identified publicly (and the likely higher number of undisclosed compromises), the paucity of reference to reparation within national cyber strategies (and the disjunction with the known, active approach taken by cyber practitioners to combat cyber security breaches[46]) is curious.

Beyond cyber security, it is common for an organization or government to provide limited detail on how it would manage consequences in the aftermath of a significant incident, when such an incident could be linked to the failure of that organization or government to take sufficient preventive action. Prevention is a predominant policy focus. Road safety is a perfect example: despite Western nations mostly having effective consequence management systems that save lives (such as ambulance networks), road safety strategies consistently do not refer to post-crash actions.[47]

The 2016 Australian Cyber Security Strategy did not refer to consequence management actions in the aftermath of a major information breach. Among more than 30 recommendations, only one touched on post-incident requirements, and even this recommendation adopted an almost exclusively preventive focus.[48] The future requirement for consequence management actions was absent (excluding a reference to the low uptake in cyber insurance), suggesting a limited focus on post-incident considerations in the strategy. Similarly, in the US, the 2018 Department of Defense Cyber Strategy barely referred to consequence management in the aftermath of a breach.[49]

To be sure, there are reasonable explanations for the lack of reference in cyber strategies to reparative actions, even though reparative actions are well embedded in many assessment and response frameworks. First, it is (obviously) better to prevent a negative event than to have to manage its repercussions.[50] Second, strategies consistently adopt a positive focus. If the public is a target audience for a strategy, one aim is almost certainly to instil confidence that the government has the ability to protect its citizens. Third, some governments may prefer to restrict knowledge of their consequence management actions, to prevent cyber-attacks impacting their recovery efforts. Finally, reparative actions in some countries are simply under-developed or even hopefully avoided.

Most of these explanations are unconvincing. Information compromises are so common now that most citizens would expect government departments to have well established clean-up strategies that are fully coordinated with broader strategies. Post-incident actions may be classified, but this would not stop them being referred to as an integral part of a strategy. Reparative actions simply should not be under-developed, given the likelihood of future successful attacks.

Perhaps most importantly, if reasonable security and resilience measures have been taken, a loss of information should not inevitably be viewed as a major failing on the part of the targeted organization. Successful intelligence collection is inevitable. If a national security community has prioritized protection for its Crown Jewels and rehearsed its reparative actions, loss of information may become an annoying reality of life, but will not undermine fundamental operating models.

No one seriously expects that there will not be major compromises of high-value information at future junctures. Without a well understood strategy incorporating information protection and consequence management actions, national security communities could be exposed as much to the post-action repercussions as they are to the actual incident, and unrealistic expectations may be created.

CONCLUSION

The technical and tactical aspects of cyber security are overshadowing more strategic consideration of information protection across national security communities. Indeed, this phenomenon is not specific to any particular security community or nation—it is widespread because there are many pressures and immediate challenges leading to this tactical approach. But as nations face sophisticated strategic competitors, their national security communities must be focused on a more comprehensive approach to protecting their most important information.

If cyber security is indeed a priority, it has presumably been given this priority because there is a need to protect national security communities' information and information links from the most serious threats. If this is true, then a broad effort to achieve wide-ranging cyber security is neither addressing the full problem nor offering an adequate structure for future threats. This impacts the efficacy of cyber security investment.

The recommended principles outlined in this paper may add to the coherence of information security plans and strategies. They are premised on the fact that a nation's key information can now be obtained in many ways, in large quantity, by a strategic competitor. It is hardly an alarmist position to predict that significant information compromises—including of classified data—are likely to occur regularly. Any national security community whose operating model requires protection of certain information for it to be successful must be clear

about what its Crown Jewels are; prioritize the protection of those Crown Jewels against specific threat intelligence; enact measures like standing deception plans to limit the benefit a strategic competitor can gain through effective intelligence collection; and develop comprehensive response and recovery plans to enhance resilience in the event of compromises and failures.

NOTES

1. The membership of most national security communities and intelligence communities is extensive. For example, see Office of the Director of National Intelligence, Members of the IC, website, https://www.dni.gov/index.php/what-we-do/members-of-the-ic, accesed une 20, 2020; Australian Government, *Australian National Security*, [website], https://www.nationalsecurity.gov.au/WhatAustraliaisdoing/Pages/NationalSecurityAgencies.aspx, accessed April 20, 2020.
2. Cyber security can be defined as the protection of networks, devices, programs and data from attack, damage or unauthorized access.
3. Department of Prime Minister and Cabinet, Australia's Cyber Security Strategy: Enabling innovation, growth and prosperity (Commonwealth of Australia, 2016), 33; Scott Morrison, $156 million to protect Australians from online attacks (Media Release, April 29, 2019), 1-2.
4. For example, Keith Joiner, "How Australia can catch up to U.S. cyber resilience by understanding that cyber survivability test and evaluation drives defense investment" *Information Security Journal: A Global Perspective* (26:2, 2017), 74-75.
5. Information links refers to networks that transfer data but are not specifically for human-to-human communications to allow the effective functioning of military equipment; for example, the uplink to control an un-crewed aerial system for flight and navigation control. For brevity, 'information and information links' will be described as 'information' in this paper.
6. This paper acknowledges 'peacetime' as a relative concept, blurring the distinction between peace, competition and conflict, but for brevity will use the term 'peacetime' to describe periods where there is no declared conflict.
7. Department of Defense, *DoD Cloud Strategy* (Washington, D.C., December 2018), 1-2.
8. Michael Kansteiner, *Mitigating Risk to DoD Information Networks by Improving Network Security in Third-Party Information Networks* (Monterey, California: Naval Postgraduate School, June 2016), xv-xvi.
9. That is, those information systems not supported as part of Defence's primary enterprise networks such as the Protected Network. See Chief Information Officer Group, 'Our Projects', Department of Defence, https://www.defence.gov.au/CIOG/Projects.asp, accessed November 15, 2019; Department of Defence, Defence Annual Report 2013-14: Volume One (Commonwealth of Australia, 2014), 51.
10. Informatech, *Our Experience*, https://informatech.com.au/projects, accessed November 18, 2019.
11. Department of Defense, Summary: Department of Defense Cyber Strategy (Washington, D.C., 2018), 2.
12. For example, 'to enable all Australians to be secure online,' See Department of Prime Minister and Cabinet, "Australia's Cyber Security Strategy: Enabling innovation, growth and *prosperity*" (Commonwealth of Australia, 2016), 3.
13. President of the United States, National Cyber Strategy of the United States of America (Washington, D.C., September 2018), 1; Department of Prime Minister and Cabinet, Australia's Cyber Security Strategy: Enabling innovation, growth and prosperity (Commonwealth of Australia, 2016).
14. David Barno and Nora Bensahel, "Why the United States Needs an Independent Cyber Force," *War on the Rocks*, May 4, 2021, https://warontherocks.com/2021/05/why-the-united-states-needs-an-independent-cyber-force/, accessed September 25, 2021.
15. Standing intelligence agency rivalries aside; for example, Manoj Shrivastava, Re-energising Indian Intelligence (Centre for Land Warfare Studies, Vij Books, India, 2013), 5; In the Australian context, see Sally Neighbour, "Hidden agendas," in *The Monthly,* November 2010, https://www.themonthly.com.au/issue/2010/november/1289174420/sally-neighbour/hidden-agendas, accessed November 15, 2019.
16. Hervé Debar, "Cybersecurity: high costs for companies,: *The Conversation*, February 4, 2019, https://theconversation.com/cybersecurity-high-costs-for-companies-110807, accessed September 25, 2021.
17. President of the United States, National Cyber Strategy of the United States of America.
18. Department of Prime Minister and Cabinet, Australia's Cyber Security Strategy: Enabling innovation, growth and prosperity (Commonwealth of Australia, 2016).
19. Australian Government, Australia's 2020 Cyber Security Strategy: A call for views (Commonwealth of Australia, 2019), 7-9; the paper referred to essential services as areas of most concern (although only incorporating services such as water providers), and this could be built upon to determine where a priority for information security could be applied.
20. Australian Signals Directorate, Annual Report 2018-19 (Australian Government, Canberra, 2019), 23.
21. Federal Communications Commission, *Cybersecurity for Small Business,* https://www.fcc.gov/general/cybersecurity-small-business, accessed June 1, 2020.

NOTES

22. Australian Cyber Security Centre, *Information Security Manual* (Australian Government, November 2019), 5.
23. Nigel Phair, "Cybersecurity strategy should focus on corporate Australia," *The Strategist*, September 27, 2019, https://www.aspistrategist.org.au/cybersecurity-strategy-should-focus-on-corporate-australia/, accessed November 15, 2019.
24. Inspector General U.S. Department of Defense, Summary of Reports Issued Regarding Department of Defense Cybersecurity From July 1, 2017, Through June 30, 2018 (Washington, D.C., January 9, 2019), 10; AustCyber, Sector Competitiveness Plan – Chapter 3 – The challenge: Australia needs to fill the workforce gap, remove startup barriers and strengthen research and development, https://www.austcyber.com/resources/sector-competitiveness-plan/chapter3, accessed April 20, 2020.
25. Jennifer Li and Lindsay Daugherty, *Training Cyber Warriors: What Can Be Learned from Defense Language Training?* (Santa Monica, CA: RAND Corporation, 2015), 1-3; Greg Austin, 'Cyber revolution' in Australian Defence Force demands rethink of staff, training and policy,' *The Conversation*, July 3, 2017, https://theconversation.com/cyber-revolution-in-australian-defence-force-demands-rethink-of-staff-training-and-policy-80317, accessed November 16, 2019.
26. Mariel Borowitz, 'War in Ukraine highlights the growing strategic importance of private satellite companies—especially in times of conflict', *The Conversation*, August 15, 2022, https://theconversation.com/war-in-ukraine-highlights-the-growing-strategic-importance-of-private-satellite-companies-especially-in-times-of-conflict-188425, accessed September 29, 2022.
27. For example, Ben Fitzgerald, 'Australia needs calibrated deterrence against cyber attacks', *The Interpreter,* December 10, 2015, https://www.lowyinstitute.org/the-interpreter/australia-needs-calibrated-deterrence-against-cyber-attacks>, accessed November 15, 2019.
28. Thomas Daemen, 'Cyber attack fear hinders progress', Microsoft, June 26, 2018, https://news.microsoft.com/en-au/2018/06/26/cyber-attack-fear-hinders-progress/, accessed November 15, 2019.
29. Indeed, the Australian Security and Intelligence Organisation recently argued that there were insufficient resources being applied to counter-intelligence. See Colin Packham, 'Australian intelligence agency wants more resources to counter foreign interference', *Reuters*, October 16, 2019, https://www.reuters.com/article/us-australia-security/australian-intelligence-agency-wants-more-resources-to-counter-foreign-interference-idUSKBN1WW05M, accessed November 25, 2019.
30. Chethan Kumar, 'Surgical Strikes: First major use of Cartosat images for Army', The Times of India, September 30, 2016, https://timesofindia.indiatimes.com/india/Surgical-Strikes-First-major-use-of-Cartosat-images-for-Army/articleshow/54596113.cms, accessed November 1, 2019; Jane's Intelligence Review, *China integrates long-range surveillance capabilities*, 2017, https://www.janes.com/images/assets/477/75477/China_integrates_long-range_surveillance_capabilities.pdf, accessed October 1, 2019.
31. Andrew Greene, 'Chinese spy Wang Liqiang alleges Beijing ordered overseas murders, including in Australia', *ABC News*, November 23, 2019, https://www.abc.net.au/news/2019-11-23/chinese-spy-wang-liqiang-seeks-political-asylum-australia-report/11732174, accessed November 23, 2019.
32. Anthony Kuhn, 'China is Placing Underwater Sensors in The Pacific Near Guam, NPR, February 6, 2018, https://www.npr.org/sections/parallels/2018/02/06/582390143/china-is-placing-underwater-sensors-in-the-pacific-near-guam, accessed October 10, 2019.
33. Pieter Velghe, 'Reading China: The Internet of Things, Surveillance, and Social Management in the PRC', in *China Perspectives* (2019(1), 86; Qiao Long, 'China Aims For Near-Total Surveillance, Including in People's Homes', *Radio Free Asia*, March 30, 2018, https://www.rfa.org/english/news/china/surveillance-03302018111415.html, accessed November 15, 2019.
34. Nikolai Novichkov, 'Russia Creates SIGINT Payloads for Granat-4 UAV', Real Clear Defense, February 17, 2016, https://www.realcleardefense.com/2016/02/18/russia_creates_sigint_payloads_for_granat-4_uav_279172.html, accessed December 3, 2019.
35. M. Taylor Fravel, 'China's "World-Class Military" Ambitions: Origins and Implications,' *The Washington Quarterly* (43:1, Spring 2020), 85-86, 95-96.
36. Sabra Lane, 'AM with Sabra Lane', *ABC News*, December 21, 2018, https://www.abc.net.au/radio/programs/am/we-will-shine-a-light:-tobias-feakin-on-chinas-cyber-spying/10645354, accessed November 15, 2019.
37. Including US assessments, such as Defense Intelligence Agency, "China Military Power: Modernizing a Force to Fight and Win" (DIA-02-1706-085, 2019), 24.

NOTES

38. Sudhansu Nayak, "Few grains from the "Thousand Grains of Sand," Observer Research Foundation, March 8, 2017, https://www.orfonline.org/expert-speak/few-from-thousand-grains-of-sand/, accessed November 20, 2019.
39. David Cooper, *Economic Espionage: Information on Threat From U.S. Allies* (United States General Accounting Office, Testimony, February 28, 1996), 1-2.
40. Damien Manuel, 'Think your metadata is only visible to national security agencies? Think again', *The Conversation*, August 5, 2019, https://theconversation.com/think-your-metadata-is-only-visible-to-national-security-agencies-think-again-121253, accessed May 2, 2021.
41. Joseph Cirincione, Jessica Tuchman Mathews, George Perkovich, with Alexis Orton, WMD in Iraq: Evidence and Implications (, Washington, D.C.: Carnegie Endowment for International Peace, January 2004), 80.
42. Angus Campbell, *War in 2025* (Speech, Australian Strategic Policy Institute International Conference, June 13, 2019), 9.
43. United States Department of Defense, *Military Deception* (Joint Publication 3-13.4, 13 July 2006), vii-viii.
44. Reparative actions and consequence management can include actions such as damage assessments, declassification of information, disposal of hardware, international liaison, media releases and mandatory reporting.
45. Ray Rothrock, 'Digital Network Resilience: Surprising Lessons from the Maginot Line', *The Cyber Defense Review*, Fall 2017, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Digital%20Network%20Resilience_Rothrock.pdf?ver=2018-07-31-093725-860, accessed September 25, 2021.
46. For example, see National Cyber Security Centre, *NCSC Cyber Assessment Framework guidance*, 2019, https://www.ncsc.gov.uk/collection/caf, accessed May 2, 2021.
47. For example, J. Wall, J. Woolley, G. Ponte and T. Bailey, "Post crash response arrangements in Australia compared to other high performing road safety nations," Proceedings of the 2014 Australasian Road Safety Research, Policing & Education Conference, Melbourne, November 12-14, 2014), 1-3.
48. Australian Signals Directorate, "Strategies to Mitigate Cyber Security Incidents" (Australian Cyber Security Centre, Australian Government, February 2017), 1-2.
49. Department of Defense, *Cyber Strategy* 2018, 3.
50. Sean Duca, "Cybersecurity: Why prevention is better than the cure," *CEO Magazine*, May 22, 2018, https://www.theceomagazine.com/business/innovation-technology/cybersecurity-why-prevention-is-better-than-the-cure/>, accessed April 20, 2020.