SPECIAL REPORT

Deterrence in cyberspace

Different domain, different rules

Liam Nevill and Zoe Hawkins

July 2016

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

ASPI

Liam Nevill

Liam is an analyst in ASPI's International Cyber Policy Centre, researching and writing on international and domestic cyber issues. Prior to joining ASPI Liam worked at the Australian Department of Defence on strategic and international defence policy issues.

Zoe Hawkins

Zoe is a researcher in ASPI's International Cyber Policy Centre, researching and writing on international and domestic cyber issues. Zoe is also working as a research assistant on the policy implications of quantum technology for the Centre for International Security Studies at the University of Sydney.

About ASPI

ASPI's aim is to promote Australia's security by contributing fresh ideas to strategic decision-making, and by helping to inform public discussion of strategic and defence issues. ASPI was established, and is partially funded, by the Australian Government as an independent, non-partisan policy institute. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

Cover image: Mushroom cloud from nuclear bomb explosion © Igor Zh. / Shutterstock.

Deterrence in cyberspace

Different domain, different rules

Liam Nevill and Zoe Hawkins

July 2016

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

First published July 2016

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

Tel + 61 2 6270 5100
Fax + 61 2 6273 9566
enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

 Facebook.com/ASPI.org

 @ASPI_org

CONTENTS

US President Barack Obama (L) chats with Chinese President Xi Jinping as they walk from the West Wing of the White House in Washington, 24 September 2015. Xi arrived in Washington for a state visit and talks with President Barack Obama expected to be clouded by differences over alleged Chinese cyber spying, Beijing's economic policies and territorial disputes in the South China Sea. © Mike Theller / Reuters / Picture Media.

INTRODUCTION

In a society that's now reliant on cyberspace for everyday life, and when everything from cars, electricity grids and dams to weapons systems is connected to a network, the potential effects of malicious or aggressive actions in cyberspace warrant some justified concern.

Cyberspace is still in its infancy as an environment of state and non-state actor competition. While it's not yet well understood how cyberspace's inherent vulnerabilities may endanger safety and even sovereignty, there's an unfortunate amount of hysteria that accompanies discussion of cyber threats and a misunderstanding of appropriate policy responses. Concerns about a coming 'cyber Pearl Harbor' or 'cyber Armageddon' arise frequently, and the term 'cyberwar' is used without consideration of what constitutes warfare and what it would look like in cyberspace.[1]

The inherent vulnerabilities of cyberspace have extended into critical domains, posing a strategic challenge to the security of the modern state and international relations in general. Protecting information, overcoming the vulnerabilities of infrastructure and adapting to increasingly networked military capabilities will be key policy priorities of the next decade. Therefore, there's an imperative to consider the nature of cyber instability and how best to respond to it.

Deterrence is often raised as an optimal policy response to cyber threats and as a solution to persistent cyber espionage. However, threatening punishment won't deter cyberattacks or other malicious behaviour, but instead is more likely to contribute to international instability. Alternative security strategies that protect national interests in cyberspace, while building confidence and reducing the risk of conflict, are vital in this context.

This paper examines the application of deterrence concepts to cyberspace, discusses cybersecurity implications for broader deterrence frameworks, and makes policy recommendations to enhance cybersecurity and strengthen broader deterrence postures.

DETERRENCE

Deterrence has been used by states throughout history as a useful way of discouraging unwanted behaviour and preventing conflict, simply through dialogue and posturing. The policy is based on the assumption that states are rational actors that make decisions through cost–benefit analysis.[2] On this assumption, one can deter a challenger by changing their decision-making calculus, increasing the perceived costs of their action (deterrence by punishment) or decreasing the expected benefit (deterrence by denial).

Deterrence by punishment features prominently in national security strategy. To establish such a policy, a defending state must first identify the 'red line' that distinguishes between behaviour it will accept and behaviour it will punish. It must then choose a suitable punishment for an actor that crosses that line. Finally, it must establish the credibility of its threat by communicating that it has the ability, resources and intent to follow through on the punishment.[3] Importantly, the selection of red lines and appropriate punishments is informed by contemporary norms and international law.

If done successfully, these threat frameworks can be used as bargaining power in international relations.[4] Deterrence can be used when an immediate issue arises, or as part of long-term 'general' policies designed to prevent acute crises from arising.[5] Most famously, deterrence by punishment played a fundamental role in the Cold War. As nuclear arsenals grew and delivery systems became more survivable, the knowledge that conducting a nuclear attack would guarantee one's own destruction, a construct referred to as 'mutually assured destruction' (MAD), maintained global stability.[6]

Alternatively, instead of raising the costs, one can influence an adversary's decision-making by withholding the perceived rewards of certain behaviour and building an international conflict reduction framework. A denial strategy involves communicating that one's defences are so robust that any aggressive efforts against them are futile. However, this defensive approach is less prominent in international relations due to the often difficult nature of its implementation and the high profile of deterrence by punishment during the Cold War. The positive and negative attributes of both strategies and their application in cyberspace are discussed in further detail below.

CYBER DETERRENCE

Cyberspace has been branded as a new front line for modern conflict and, as in the rise of air power doctrine in the 20th century, attempts to define its role and utility in warfare draw on the experience of familiar conflicts and policy. This has resulted in the transposition of strategies from traditional mediums of conflict to the digital domain.

The success of deterrence by punishment in the Cold War has clearly informed the public dialogue on policy approaches to managing cyber threats to national security, as the theme of retaliation is common in national cyber policies. Australia's recent Cyber Security Strategy, released in April 2016, claims that 'Australia's defensive and offensive cyber capabilities enable us to deter and respond to the threat of cyber attack'. At the strategy's launch, Prime Minister Turnbull further emphasised that 'acknowledging this offensive capability, adds a level of deterrence'.[7]

Australia's recent Cyber Security Strategy, released in April 2016, claims that 'Australia's defensive and offensive cyber capabilities enable us to deter and respond to the threat of cyber attack'.

This rhetorical trend is evident globally. The 2011 US International Strategy for Cyberspace describes plans to 'ensure that the risks associated with attacking or exploiting our networks vastly outweigh the potential benefits'.[8] More recently, the 2015 US Cyber Command vision paper, *Beyond the build,* also identified enhanced offensive and defensive cyber capabilities as an essential part of America's strategy to 'deter or defeat enemies in cyberspace'.[9]

Similarly, UK Chancellor George Osborne has argued that establishing a cyber deterrent involves 'making sure that whoever attacks us knows we are able to hit back'.[10] The 2015 UK National Security Strategy and Strategic Defence and Security Review goes further, warning that 'We will treat a cyberattack on the UK as seriously as we would do an equivalent conventional attack, and we will defend ourselves as necessary.'[11]

However, Australian, US and UK conceptions of deterrence in cyberspace also identify the importance of cyber stability achieved through defensive posturing. For example, the 2015 US Department of Defense (DoD) Cyber Strategy places an emphasis on network defence and resilience, stating that the first of the DoD's three primary cyber missions is to 'be able to secure its own networks against attack and recover quickly if security measures fail', adding that 'Network defense operations on DoD networks constitute the vast majority of DoD's operations in cyberspace.'[12] Similarly, the UK's 2015 review outlines intentions to 'introduce stronger defences for our systems.'

Australia's Cyber Security Strategy also acknowledges the strategic value of cyber defences, arguing that robust cybersecurity measures 'can also be an effective deterrent by increasing the effort necessary for an attacker to succeed'.

These government statements are attempts to pursue cyber stability by covering all bases, including elements of both the punishment and the denial approaches. This demonstrates the complexity involved in applying deterrence concepts to cyberspace. Unfortunately, it also reveals that governments are applying conventional theories to the digital domain without carefully considering their suitability or the consequences.

States have an inherent right to respond to attacks on their national security, including acts conducted in or through cyberspace that cause significant death or destruction. However, making threats to deter cyber actions is more challenging than in the physical domains, complicating the development of appropriate responses.

This paper suggests that alternative approaches such as bolstering cyber defences and confidence building are far more effective in scenarios in which the goal is simply to maintain cyber stability. The following section addresses the significant issues that arise when applying deterrence by punishment strategies to cyberspace and the risk to international stability that making such statements incurs.

DETERRENCE BY PUNISHMENT IN CYBERSPACE

Constructing a deterrent threat framework requires a variety of steps, all of which are more challenging, some near impossible, in cyberspace. This section delineates the conceptual obstacles policymakers will face when attempting to establish a cyber deterrent through punishment. In addition, the difficulties posed by contextual realities, such as rising state and non-state actors, are addressed. Together, these challenges render the deterrent by punishment strategy not only ineffective, but potentially escalatory and a threat to global stability.

Conceptual obstacles

The main conceptual obstacles that policymakers face when trying to establish a cyber deterrent are establishing thresholds, communicating threats, detecting intrusions and attributing responsibility.

Thresholds

Articulating a clear distinction between acceptable and unacceptable behaviour is essential in order to establish an unambiguous 'red line' that defines the boundaries of a deterrence policy. For example, the sanctity of sovereign territory is a black and white concept, such that invasion of a state's territory by a foreign power justifies counterattack in self-defence using all appropriate means of national power. However, developing and applying deterrence policy to cyberspace is made difficult by the extensive spectrum of potential acts in cyberspace, as shown in Figure 1.

Figure 1: Spectrum of potential acts in cyberspace

Although 'cyberattack' colloquially refers to just about any malicious action in cyberspace, for the purposes of deterrence policy it must be more clearly defined. In line with existing normative practice, the term 'cyberattack' should only be used to describe an action in or through cyberspace that causes physical destruction or loss of life.[13] Other malicious acts, such as cybercrime, hacktivism and cyber espionage all fall short of this threshold of violence and complicate the application of conventional thresholds to cyberspace. The fact that cyber capabilities aren't as conveniently binary as other capabilities creates confusion over where to draw the line between what's simply a nuisance and behaviour that must be punished. However it's this grey zone of malicious cyber behaviour that also needs to be addressed in national security policy, presenting a significant challenge for policymakers.

Making threats

Choosing the appropriate punishment for malicious cyber behaviour and communicating the threat of punishment are extremely challenging. 'Just war' principles include the concept of proportionality; that is, the retaliation must reflect the scale and scope of the original act.[14] Maintaining proportionality is not only important in order to comply with international law, but also in drawing a direct connection between the behaviour and the punishment so as to reinforce the deterrence policy.[15] The threat must be effectively communicated to make an adversary aware of the defender's capabilities and its willingness to use them.[16] This is normally achieved relatively easily through threat rhetoric and the demonstration of the state's power in military exercises, weapons tests and involvement in other conflicts. In this way, a potential adversary can observe the state's capability to make good on its threats and is more effectively deterred from their original course of action.

Explicitly communicating one's capacity to exact a like-for-like punishment would be likely to prompt the adversary to patch their relevant weaknesses in cyberspace, thus nullifying the capability altogether.

However, threatening a proportionate *retaliation within cyberspace* is made difficult by the confidential nature of cyber capabilities. Cyberweapons rely on the exploitation of vulnerabilities in an adversary's network, and a state's capability to punish is thus often defined by features of which the adversary is unaware, making them single-use capabilities.[17] Explicitly communicating one's capacity to exact a like-for-like punishment would be likely to prompt the adversary to patch their relevant weaknesses in cyberspace, thus nullifying the capability altogether.

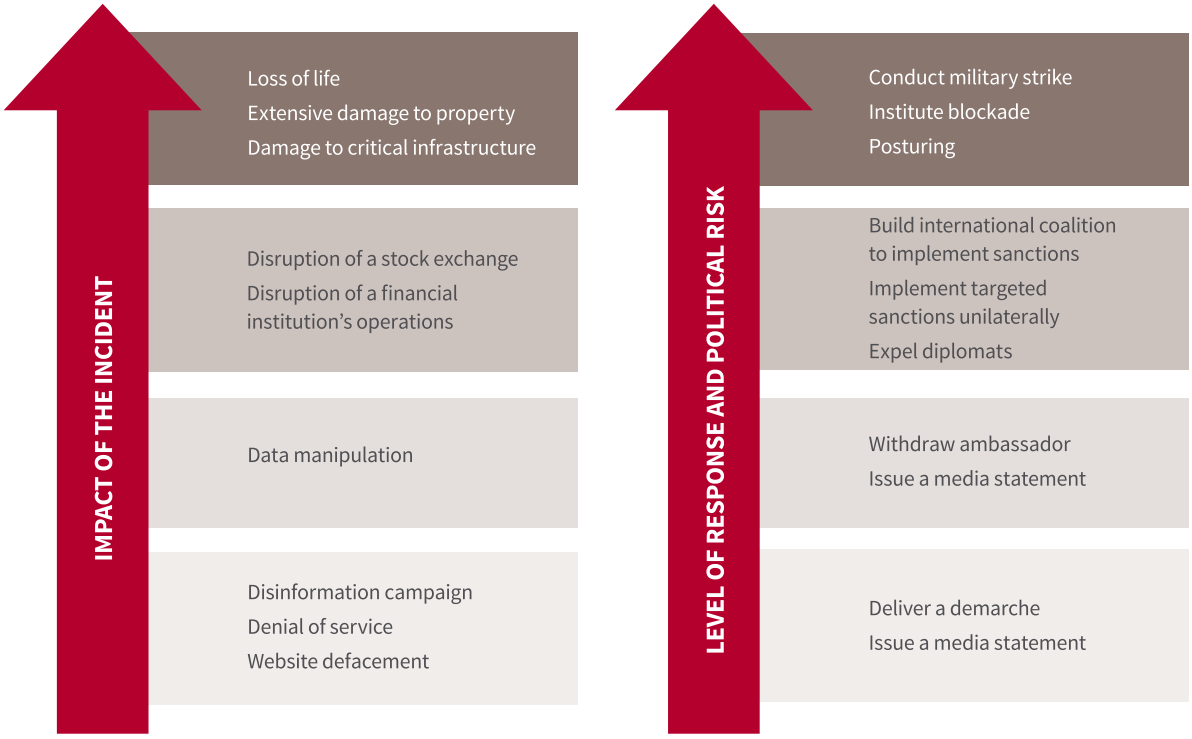
Moreover, offensive cybertools are often highly discriminate and tailored for each individual target. As such, they can't always be used as a one-size-fits-all threat—an issue referred to by Thomas Rid as 'the problem of generics'.[18] While threatening cyber retaliation through rhetoric is possible, it falls far short of the credibility generated through demonstrable capabilities. The necessarily low visibility of cyber capabilities means it's difficult to construct a credible declaratory policy around one's cyber retaliation capabilities. Since deterrence is founded on both an actor's ability to deliver the threatened punishment and their will to do so, difficulty in communicating cyber capabilities can lead to an over-reliance on aggressive rhetoric (the risks of unintentional escalation associated with this approach are addressed below).

Committing to *retaliate outside of cyberspace* is also challenging because of the absence of established normative response frameworks. There are various instruments of state power available, from conventional military capabilities, including kinetic strikes (such as the infamous 'missile down your smokestack' threat), to economic sanctions or the expulsion of diplomats. However, this broad response toolkit exists without a clear global consensus on what a conventional response to a cyber incident should look like. Proportionality has been identified as an important principle for cyberspace interactions; however, without agreement on what constitutes an appropriate response to cyber acts of differing severity or even how to distinguish between them, international cyber norms remain fluid and unpredictable.[19]

There have been efforts to establish frameworks that identify proportionate real-world responses to a variety of cyber incidents, as illustrated in Figure 2.[20]

However, they are yet to be officially adopted and integrated into international normative behaviour. Until that occurs, the logic of such frameworks bears little weight on the effectiveness of cyber deterrence.

Figure 2: Policy responses to escalating state-sponsored cyber incidents



Source: Tobias Feakin, *Developing a Proportionate Response to a Cyber Incident*, Council on Foreign Relations, online.

Detecting intrusions

Deterrent threats are undermined if the act of crossing the chosen threshold isn't punished consistently. Unfortunately, the difficulty of detecting all malicious events that affect a network means that there are likely to be many intrusions that go unpunished.

Online actors are finding strategic value in launching low-intensity attacks at a high frequency.[21] This approach offers them several benefits: first, the malicious acts may go unnoticed; second, any single act that's detected is likely to fall below an adversary's threshold for retaliation and outside their punishment framework. Despite often being inconsequential in isolation, these acts can be used as part of a high-volume strategy, often referred to as 'salami-slicing', that constitutes a broader strategic campaign that has cumulative detrimental effects in the long term. In this model, the credibility of a threat is undermined by an adversary's perception that their action will probably either not be noticed or not trigger a response.

Furthermore, the immediacy of a punishment directly correlates with its effectiveness in establishing a deterrent. The longer the time lapse between the crossing of a red line and the associated retribution, the less apparent the connection between the two for both the punished actor and the international community. Thus, a defender's ability to establish deterrence by punishment in cyberspace is inhibited by the challenges of detecting serious infractions quickly enough.[22]

Without adequate measures to detect most cyber incidents, retaliation that does take place may also appear to be conducted at random. Such inconsistency confuses thresholds and reduces the credibility of the deterrence posture. This disparity among the broad range of potential actions in cyberspace, weak detection and unclear response frameworks is yet to be reconciled.

The difficulty of attribution

When a cyber incident is detected, the difficulty of accurately attributing responsibility makes it hard to establish a credible deterrent threat. An essential feature of deterrence is a challenger believing that they will be identified and punished. Effectively executing attribution and punishment offers multiple benefits, such as strengthening the existing deterrence framework and improving collective security.[23] This process is often relatively easy in the physical domain, where evidence such as trajectory analysis or national markings on equipment and personnel make the guilty party obvious.

Unfortunately, the same process is comparatively challenging in cyberspace. Networks weren't designed with attribution in mind, and unfortunately cyberspace favours anonymity. To make things worse, many techniques can be used to mask the source of an attack, including botnets, proxy servers and onion routing.[24] Cyber forensics can be used to try to identify a perpetrator, but this process is often slow, unreliable and even impossible. Even if it's possible to identify the particular computer or IP address that's the source of an attack, that doesn't offer any conclusive evidence about the identity, intent and associations of its user. The inherent uncertainty of attribution was demonstrated by the hacking of French television channel, TV5 Monde, in April 2015. The sophisticated incident was initially pinned as an act of Islamic State, and was only later found more likely to be the handiwork of Russian-based hackers.[25]

The desirability of attribution

Following through on a threat is central to maintaining a deterrent, but retaliating against the wrong actor may be more harmful than helpful. In an effort to retain deterrence credibility, it's been suggested that, even if unsure, states should 'assign responsibility' to those states or organisations connected to the event.[26] However, accidentally punishing an innocent party risks generating a new enemy, escalating tensions and potentially causing a net decrease in cybersecurity. Incorrect attribution also erodes the deterrent effect, because 'if innocence does not matter, why be innocent?'[27] Misplaced punishment will not only affect the future decision-making calculus of the wrongly accused, but also that of third-party observers who deem the attribution to have been unfounded. For this reason, attribution and retaliation are not only difficult, but also risky.

Even when one has properly identified the culprit, it may still be a strategically sound choice not to pursue attribution and punishment. As mentioned above, the consensus of onlookers is an important feature of deterrence. A high level of public attribution is necessary to convince the culprit and the international community that the retaliation is justified and acceptable within the bounds of the UN Charter.[28] Doing so may require a state to reveal valuable information on its own cyber capabilities and its access to foreign networks. Disclosing that kind of information may decrease one's ability to defend against, or track, potentially more harmful incidents in the future. This difficulty is compounded by the potential for an adversary to be confident that, even if identified, they could still cast enough doubt over the accuracy of the attribution in the eyes of the international community to erode the credibility of the defender's broader deterrence framework. So, defenders must make a judgement on the relative value of the attribution and its cost to their long-term strategic advantage. For this reason, attribution has been described as a double-edged sword.[29]

The risk of escalation

Basing a cyber deterrence policy on threat frameworks raises the risk of escalating conflict unintentionally or unreasonably. Once a threat of retaliation is made, a state is caught in an unfavourable 'credibility–stability paradox', see box.

Faced with that choice, many states would prioritise their own credibility and risk escalating international tensions. This would have a detrimental impact on cyber stability in the long term. Cyberspace is already perceived to be an offence-dominant domain, based on the idea that its unique characteristics inherently benefit the attacker. The difficulty of plugging all network vulnerabilities, and the temporal advantage associated with proactively

developing targeted cyber 'weapons', have generated the view that it's 'cheaper and easier' to initiate an attack on an adversary than it is to defend your own networks.[30] Unintended escalations could promote the 'cult of the cyber offensive', increasing the appeal of the first-strike advantage and encouraging pre-emptive cyber offences.[31]

The Credibility–Stability Paradox

The reliability of the state's commitment to enforcing its own deterrence policy statements is a significant symbol of its political and military power. If it doesn't back up a threat when the red line is crossed, it directly reduces its credibility in the eyes of the international community, undermining its ability to both intimidate and negotiate in the future.

Conversely, making good on a threat in cyberspace can have drastic impacts on international stability. The full impact of an action taken in cyberspace is difficult to control or predict. Therefore, the retaliation may spiral beyond the intended punishment, inflicting damage over and above what would be considered a proportionate response to the breach of a threshold. This risks a minor incident triggering a tit-for-tat escalation and 'cascading an attack in cyberspace into a much bigger conflict'.[32] This danger is exacerbated by the risk of inadvertently punishing the incorrect actor. Incorrect attribution could trigger unnecessary escalation with a third party while the real aggressor goes unpunished and undeterred.

Thus, once such a cyber deterrence framework's constructed, a state faces the strategic dilemma of being forced to choose between maintaining its credibility and the risks of collateral damage.

Source: Singer, P.W. & Friedman, Allan. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2013, p. 137.

This isn't to say that offensive cyber capability shouldn't be developed, but rather that it shouldn't be developed for the purpose of making threats. Offensive cyber capabilities have the potential to enhance a state's military potency when used to achieve or support military effects, but they are unlikely to facilitate the establishment and maintenance of cyber stability through deterrence by punishment for the reasons outlined in this paper.

International discussions on the application of international law to offensive cyber actions and the role of restraint can offer positive diplomatic value. Policy transparency of this kind will help generate stronger normative frameworks, reduce the risk of international misunderstandings and support a more stable cyberspace. Note that there's a clear distinction between such constructive policy dialogue and the aggressive use of threats for the sake of intimidation.

Conversely, rhetoric on the efficacy of one's defensive capabilities does have a direct link to the strength of national deterrence posturing (a concept that's addressed below).

Contextual obstacles

In addition to conceptual and doctrinal barriers to cyber deterrence, the absence of a settled framework for cyber relations and the proliferation of violent non-state actors are challenging contextual obstacles.

Norm development and global power shifts

Explicit contradictions between the vision of liberal democratic states and that of reformist rising powers for the future of cyber relations make cyber norm development an increasingly fragmented process.[33] This is evident in UN processes such as the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, otherwise known as the UNGGE.[34]

Cyberspace is likely to remain a proxy battleground for broader geopolitical tensions between the US and emerging powers. As a result, an established, universally accepted framework for cyber relations is unlikely to emerge in the near future.

A plurality of actors

These concepts become even more challenging when surveying the contemporary realities of international relations. While non-state actors have been present for years, in recent times their number and influence in global politics have grown. Deterring violent non-state actors (VNSAs) in cyberspace is especially challenging due to the domain's strategic value, VNSAs' relatively low vulnerability to retaliation and their position outside the Westphalian international structure.

> Violent non-state actors are relatively immune to punishment based on deterrence policies, as they don't have territory, fixed military or civil assets or societies that can be held at risk by another actor.

Access to cyberspace is simple and cheap, offering VNSAs that possess comparatively low hard-power resources a flexible medium in which to create disturbance, distribute propaganda and gain global notoriety. For those reasons, it will be considerably difficult to deter VSNAs from exploiting the advantages of cyberspace.

Deterrence by punishment between states is focused on threatening the military capability, infrastructure or populations of an adversary so as to discourage them from taking an unwanted action. In contrast, VNSAs are relatively immune to punishment based on deterrence policies, as they don't have territory, fixed military or civil assets or societies that can be held at risk by another actor.[35] The asset asymmetry between states and VNSAs limits VNSAs' suitability as targets of deterrent threats.

VNSAs are also relatively impervious to traditional deterrence threats, as they possess a fundamentally different value-set from state actors.[36] As mentioned above, the importance of behavioural norms and the rule of law to the international community plays an important role in state-on-state deterrence. In contrast, VNSAs are often more concerned with gaining public notoriety and grassroots support. Therefore, soft power considerations of credibility and diplomatic capital that normally constrain state behaviour may have less impact on their decision-making. In fact, it's been argued that some VNSAs would benefit strategically from the international acknowledgement and potential sympathy that would be generated by a counterattack from the US, for example.[37]

Various obstacles make deterrence by punishment not only difficult in cyberspace, but also destabilising. Conceptual issues of thresholds, proportionality, messaging, attribution and escalation are further exacerbated by the contextual difficulties of dealing with reformist states and VNSAs. If the goal is achieving Cold War-era stability in cyberspace, then committing to cyber threats may be a counterproductive strategy. Instead, states should recognise the strategic value of peaceful engagement in cyberspace and adopt alternative approaches that support international stability.

ALTERNATIVE APPROACHES

The practical difficulties of deterring cyber adversaries through threats of punishment suggest that it's necessary to find a different approach to protect our interests in a stable and secure cyberspace. Options include denial, dissuasion, conflict prevention and confidence building.

Denial

In contrast to punishment approaches, denial approaches seek to lower the benefit of an action rather than raise the cost. Sophisticated contemporary cyber strategies such as that of the US DoD referred to above incorporate both punishment and denial approaches. Paul K Davis of RAND defines denial or dissuasion as:

> Dissuading an action by having the adversary see a credible capability proven to prevent him from achieving potential gains adequate to motivate the action.[38]

Implementing a denial strategy in cyberspace requires strong, adaptive defences, resilient networks, and the use of other advanced techniques and technology to reduce the perceived value of malicious behaviour. Denying enemies an advantage commensurate with the effort required to breach security should dissuade them from further attempts on the network. This supports cybersecurity generally and, if effectively conducted, can further enhance conventional deterrence postures, improving a state's overall national security.

New security technologies

While adversaries become more sophisticated in their exploitation of cyberspace, so too do innovative security technologies that prevent or detect network entry and protect critical data. Continuing to invest in those defences and generating a 'defence in depth' will help prevent the theft of information or the sabotage of one's networks, reducing the benefits for malicious actors.[39]

Next-generation firewalls are now capable of deeper, application-level inspection, assessing not only the safety of the origin of incoming data packets but also their content.[40] Within a system, the integrity of sensitive data can be protected through encryption technologies to further decrease the value an adversary can gain from a cyber intrusion. There's a significant amount of research into the refinement and improvement of encryption processes, which are evolving from classic technologies to more complex ideas such as quantum key distribution, which is 'theoretically completely secure from tapping'.[41]

Beyond conventional boundary defence type cybersecurity measures, increasingly proactive measures that can be taken within one's own network are being developed and implemented to protect critical information. Diverting an adversary's efforts, depleting their resources, planting false information and gathering intelligence can all be achieved within one's own defences in order to successfully 'shift the balance of power in CND (computer network defence)'.[42] The US Defense Advanced Research Projects Agency (DARPA) defines this strategy as 'active defence', in which the network owner engages with an intruder before and during the execution of a cyber incident.[43] These automated technologies 'interdict, isolate or remove threat vectors', denying benefits and deceiving adversaries.[44]

Resilience

Any cybersecurity measure is fallible, however, so it's critical to develop, implement and practise recovery plans that quickly re-establish operational capacity. Cyber resilience helps to balance the cost–benefit calculation in favour of the defender. Quick detection, system redundancy and fast recovery can limit the strategic impact of an incident and thus deny the enemy their desired effect.[45] Approaches to resilience should also be included in the cybersecurity considerations of the technology acquisition cycle, building in redundancies that better enable an organisation to quickly recover from a breach. A denial approach to dissuading or deterring an adversary's actions in cyberspace has the additional value of providing a tangible defensive solution, should deterrence fail and an aggressor decides to act.[46]

The limitations of a denial strategy

These denial approaches will have a cumulative effect, as adversaries are gradually convinced of the futility of their actions. While the number of attempts to breach network security may decline only slowly in the near term, the number of successful attempts should diminish in the long term. Further, a denial strategy might not dissuade a very sophisticated or patient opponent that the reward isn't worth the effort to enter a network. However, it should make it easier to identify the persistent actors by weeding out the 'noise' of other less potent cyber adversaries as they gradually move on to less difficult targets. See Table 1.

Conflict prevention and confidence building measures

Efforts to build greater understanding of and confidence in state and private activity in cyberspace are underway in bilateral and multilateral dialogues globally. Establishing normative frameworks and building confidence in the mutual benefits of complying with agreements and norms of behaviour will help reduce the risk of cybersecurity incidents entering an escalatory spiral of punishment and counter-punishment.

Norm development

The lack of agreed behavioural standards in cyberspace poses an increasingly acute threat to stability. Norms offer a solution to this issue, offering the potential to bring 'predictability, stability and security to the international environment'.[47] Work to develop agreed norms for cyberspace is underway at the global and regional multilateral levels as well as between key actors in cyberspace, particularly the US, China and Russia.

Establishing norms in cyberspace won't be a straightforward process as reformist actors challenge existing international norms as part of a broader shift in global power politics. America's unipolar moment is giving way to a multipolar world, and that has serious implications for the survival of today's international norms. China and Russia are both challenging accepted norms in political, military and economic arenas, testing the limits of the status quo. Cyberspace is a new environment that's more easily shaped by the interests of rising or resurgent powers than domains that have long-established legal and normative frameworks.

However, that doesn't mean that this work's without merit or value—in fact, quite the opposite. The most recent UNGGE agreed to several norms that are a basis for future work to manage state relations in cyberspace, as has the Shanghai Cooperation Organisation.[48] Similar agreements have been reached bilaterally between the US and China.[49]

Private organisations are also involved in this discussion—a critical issue, considering the predominantly private ownership of cyberspace. Microsoft in particular has been active in this field, developing a suggested list of six proposed norms intended to limit conflict in cyberspace.[50]

The implementation of these agreements and the acceptance of proposals such as Microsoft's will take time but have the potential to stabilise the environment and reduce the risk of cyber conflict.

Table 1: Deterrence in cyberspace

Challenge	Deterrence by Punishment	Deterrence by Denial
Thresholds	There is a large, continuous spectrum of malicious behaviour possible in cyberspace. In order to threaten a punishment, policymakers must decide where the red line between acceptable and unacceptable cyber behaviour should be drawn. This is made difficult by the lack of international normative frameworks to inform, or give credibility, to such a distinction.	Identifying the threshold of what should be protected is an independent, values-based process. It is determined by the inherent priorities of the defending actor. The absence of norms is not an obstacle for this approach, as defence strategies require no international consensus.
Proportionality	Identifying appropriate punishments to acts in cyberspace is hindered by the underdeveloped nature of international norms. To uphold the credibility of a deterrent, the retaliation must be perceived as just by the international community. This is hard to achieve in the absence of international agreement on what is proportional.	The principle of proportionality does not apply to concepts of deterrence by denial. It is the inherent right of any actor to apply stringent defences to their assets. Thus, states are not limited in how much they can defend, in the same way that they are limited in how much they can punish.
Messaging	Messaging is challenging if one intends to retaliate in cyberspace. Offensive cyber capabilities often rely on the exploitation of unknown vulnerabilities in an adversary's network, or user error that cannot be assured to occur. Thus, articulating one's cyber threat would simultaneously undermine it by alerting the adversary to the weakness. Messaging on conventional responses is less problematic, but lack of care in making threats that cannot be followed through risks credibility.	Messaging the strength and resilience of one's cyber networks can be achieved through declaratory policy and the accumulated effect of unsuccessful attempts to breach security.
Attribution	In order for an adversary to be deterred by a threat of punishment, they must believe they will be caught. However, attribution is difficult in cyberspace, so actors are likely to proceed assuming they will either go unnoticed or unidentified. Attribution is also risky, as punishing the wrong actor can undermine the credibility of a deterrence policy.	The focus of this strategy is the effectiveness of one's defences. Thus, the identity of an adversary that attempts to intrude is not a vital component to effective deterrence.
Escalation	If deterrence fails, a defending actor faces the 'credibility-stability paradox'. They must either renege on their threat, sacrificing their credibility, or follow through on their punishment, risking international stability. Retaliation in cyberspace poses a significant threat to stability, due to the unpredictability of the scope of a cyber retaliation, and the risk of inaccurate attribution.	If deterrence fails, the damage can be limited to purely the incident that occurred. Any damage to credibility will be less public and may be re-established over time with updated defences. This policy does not risk escalation.
Plurality	Threats to retaliate in cyberspace are complicated by the specificity of capability required, thus one cannot apply the same threat to all states or actors. Threats to retaliate outside of cyberspace are also limited by the activity of VNSAs, who do not have the same territorial, economic, political or social asset and value structures to be held at risk. The rise of reformist states also poses a challenge to the stability of the domain.	Deterrence by denial is indiscriminate in its application. The effectiveness of one's network defences applies to all potential threats.

Conflict prevention and confidence building measures

Other practical measures to prevent conflict and build confidence among cyberspace actors are also an important part of the establishment of cyber stability. Such activities are being undertaken in global and regional bodies such as the ASEAN Regional Forum, which has focused on practical measures to build confidence among member states, such as table-top exercises of national and regional responses to cyber incidents. In addition, Track 1, 1.5 and 2 discussions involving state and private sector representatives are taking place globally.[51]

These discussions on national policies and strategy, perspectives on international issues, and terminology and concepts such as 'attack' and 'use of force' in cyberspace serve to build awareness and understanding of how other states view cyber incidents. The resulting clarity on national policies and response frameworks will enable national cybersecurity personnel and policymakers to cooperate and coordinate, and to pre-empt cybersecurity incidents that threaten international stability.

CYBERSECURITY AND BROADER DETERRENCE POSTURE

Cyberspace plays an important role in a state's ability to maintain its national security and military capability. While making threats against potential adversaries is unlikely to deter them from conducting cyber espionage or attacks, policy statements and actions in cyberspace must convey the state's commitment to taking strong action to secure its cyber interests if necessary. This should include national statements referencing a strong defensive cyber posture, the ability to identify major threat vectors and actors, and the ability to remain militarily potent when access to cyberspace is denied or degraded. This will sustain the credibility of the state's overall deterrence policy and posture.

Offensive cyber capabilities designed to cause injury, death, damage or destruction have the potential to enhance the capability of armed forces by contributing to overall military success. In doing so, they contribute positively to broader deterrence capability by reinforcing the lethality and effectiveness of armed forces as a tool of state power. One of the advantages offered by offensive cyber capabilities in warfare is their ability to enable conventional military operations at less risk and possibly with fewer assets by blinding defences and slowing any response by the opponent.[52]

This has two effects. First, it enhances the effectiveness of conventional punishment frameworks. Messages to potential adversaries that *offensive* cyber capabilities would be used, in accordance with international law, to enable and support conventional military forces adds weight to conventional deterrence messaging without the destabilising effect that threats of an-eye-for-an-eye cyber punishment could induce.

Second, if an actor believes that it's possible to conduct cyberattacks that interfere in the state's response to a conventional attack, that may alter their decision-making calculus and induce them to undertake military actions that they may have otherwise declined. As a result, failing to present a strong *defensive* cybersecurity posture could degrade the credibility of the state's conventional and, in severe cases, even nuclear deterrent capabilities. Continued investment in national cyber defences, intrusion resilience and the capacity to operate in a degraded cyber environment should enhance the state's overall national deterrence posture.

As noted above, the state's abilities must be communicated to have any effect on opponents' actions and decision-making. The state should convey to potential adversaries that it can launch networked conventional offensives and resist cyber intrusions in its most critical networks.

POLICY RECOMMENDATIONS

- *Avoid* constructing cyber deterrence threats. They are ineffective, carry significant risk of collateral damage and are destabilising due to the credibility–stability paradox. Statements within declaratory policy about the state's commitment to defend itself in cyberspace are necessary to support the overall deterrence posture, but on their own can't deter cyberattack or cyber espionage.
- *Encourage* the development of international norms that will help frame the discussion and inform international opinion.
- *Participate* in efforts to establish frameworks that seek to prevent conflicts in cyberspace emerging or escalating. Maintaining an open diplomatic dialogue on cyber incidents has significant potential to de-escalate potential future cyber tensions or conflict.
- *Focus* investment on capabilities that strengthen network defences and reduce the perceived value of cyber intrusions. A strong, agile and multilayered cybersecurity approach will have a greater dissuasive effect than the threat of punishment.
  - Consistent defeat or mitigation of network intrusions should re-establish the dissuasive quality of a denial strategy, messaging opponents through practice that the network is a hard target, and undermine the confidence of an adversary planning to use destructive or manipulative cybertools to support military or national objectives.
  - Altering the cost–benefit calculation in favour of the defender won't guarantee the impregnability of a network, but should make it a less attractive target and weed out 'noise' from less determined adversaries, leaving the state to focus on only the most persistent threats.
- *Invest* in resilient networks and infrastructure so that, even if the messaging fails to dissuade an adversary from taking malicious action, the systems recover quickly and little damage is done.
- A denial strategy will be similarly effective for *private sector* organisations. Investment in cybersecurity capability should be benchmarked against an assessment of the sensitivity of the data held or in transit and the risk profile of the organisation. This will ensure that capability is commensurate with threat and risk.

NOTES

1 Kim Zetter, 'Is cyber-Armageddon upon us? 3 glitches today have some saying yes', *Wired*, 8 July 2015, online; Elisabeth Bumiller, Thom Shanker, 'Panetta warns of dire threat of cyberattack on US', *New York Times*, 11 October 2012, online.

2 Frank Zagare, 'Reconciling rationality with deterrence: a re-examination of the logical foundations of deterrence theory', *Journal of Theoretical Politics*, 2014, 16(2):109.

3 William Kaufmann, *The requirements of deterrence*, Princeton University Press, 1954, p. 7; Amir Lupovici, 'Cyber warfare and deterrence: trends and challenges in research', Military and Strategic Affairs, 2011, 3(3):50.

4 Thomas Schelling, *Arms and influence*, Yale University Press, 1966, p. xiii.

5 Paul Huth, 'Deterrence and international conflict: empirical findings and theoretical debates', *Annual Review of Political Science*, 1999, 2:27.

6 Patrick Morgan, 'History: deterrence in the Cold War', in *Deterrence now*, Cambridge University Press, 2003, pp. 1–8.

7 Australian Government, *Australia's Cyber Security Strategy: enabling innovation, growth & prosperity,* 2016, online; 'Launch of Australia's Cyber Security Strategy', transcript, 21 April 2016, online.

8 US Government, *International Strategy for Cyberspace: prosperity, security, and openness in a networked world*, May 2011, online.

9 US Cyber Command, *Beyond the build: delivering outcomes through cyberspace*, 3 June 2015, online.

10 George Osborne MP, 'Chancellor's speech to GCHQ on cyber security', 17 November 2015, online.

11 UK Government, *National Security Strategy and Strategic Defence and Security Review 2015: a secure and prosperous United Kingdom*, 23 November 2015, p. 24, online.

12 US Department of Defense, *The DoD Cyber Strategy*, April 2015, online.

13 Thomas Rid, 'Cyber war will not take place', *Journal of Strategic Studies*, 2012, 35(1):7.

14 Jean-Marie Henckaerts, Louise Doswald-Beck, *Customary international humanitarian law*, volume 1, Rules, Cambridge University Press, 2005, p. 46.

15 Thomas Schelling, *Arms and influence*, pp. 149–150.

16 Lupovici, 'Cyber warfare and deterrence: trends and challenges in research', p. 51.

17 'What is a zero-day exploit?', *FireEye*, no date, online.

18 Rid, *Cyber war will not take place*, p. 51.

19 Michael Schmidt (ed.), *Tallinn manual on the international law applicable to cyber warfare*, Cambridge University Press, 2009, p. 61.

20 Tobias Feakin, 'Developing a proportionate response to a cyber incident', *Cyber Brief*, Council on Foreign Relations, August 2015, online.

21 Sean Watts, 'Low intensity computer network attack and self-defense', *International Law Studies*, 2010, 87:60.

22 Will Goodman, 'Cyber deterrence: tougher in theory than in practise', *Strategic Studies Quarterly*, 2010, 102:107.

23 Thomas Rid, Ben Buchanan, 'Attributing cyber attacks', *Journal of Strategic Studies*, 2015, 38:27–28.

24 W Earl Boebert, 'A survey of challenges in attribution', in *Proceedings of a workshop on deterring cyberattacks: informing strategies and developing options for US policy*, National Academies Press, 2010, pp. 43–46.

25 Lichfield, John. 'TV5Monde hack: 'Jihadist' cyber attack on French TV station could have Russian link'. *Independent*. 11th June 2015, online.

26 Goodman, 'Cyber deterrence: tougher in theory than in practise', p. 109.

27 Martin Libicki, 'Cyber deterrence and cyberwar', *RAND Project Air Force*, 2009, p. 41.

28 Forrest Hare, 'The significance of attribution to cyberspace coercion: a political perspective', *4th International Conference on Cyber Conflict*, 2012, p. 136.

29 Jonathan Solomon, 'Cyberdeterrence between nation-states: plausible strategy or pipe dream?', *Strategic Studies Quarterly*, 2011, 2: 8.

30 Jan van Tol, Mark Gunzinger, Andrew Krepinevich, Jim Thomas, *AirSea battle*, Centre for Strategic and Budgetary Assessments, 2010, p. 35.

31 PW Singer, Allan Friedman, 'Cult of the cyber offensive: why belief in first-strike advantage is as misguided today as it was in 1914', *Foreign Policy*, 15 January 2014, online; PK Davis, 'Deterrence, influence, cyber attack, and cyberwar', *New York University Journal of International Law and Politics*, 2014, 47(2):327–355, p. 13 online.

32 PW Singer, Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2013, p. 137.

33 Emilio Iasiello, 'Is cyber deterrence an illusory course of action?', *Journal of Strategic Security*, 2014, 7(1):57.

34 Dave Clemente, *Compelled to control: conflicting visions of the future of cyberspace*, special report, ASPI, Canberra, October 2013, online.

35 Stephen J Lukasik, 'A framework for thinking about cyber conflict and cyber deterrence with possible declaratory policies for these domains', in *Proceedings of a workshop on deterring cyberattacks: informing strategies and developing options for US policy*, National Academies Press, 2010, p. 103.

36 Iasiello, 'Is cyber deterrence an illusory course of action?', p. 62.

37 Singer, Friedman, *Cybersecurity and cyberwar: what everyone needs to know*, p. 136.

38 Davis, 'Deterrence, influence, cyber attack and cyberwar', p. 333.

39 Wei, 'The challenges of cyber deterrence', p. 18.

40 'Next-generation firewalls', *Gartner IT Glossary*, no date, online.

41 Cindy Hurst, 'The quantum leap into computing and communication', *Joint Force Quarterly*, 2015, 77:44–50.

42 Kristin Heckman, Frank Stech, Roshan Thomas, Ben Schmoker, Alexander Tsow, *Cyber denial, deception and counter deception: a framework for supporting active cyber defense*, Springer, 2015, p. 1.

43 Angelos Keromytis, *Active cyber defense (ACD)*, Defense Advanced Research Projects Agency (DARPA), no date, online.

44 Scott Jasper, 'Deterring malicious behaviour in cyberspace', *Strategic Studies Quarterly*, Spring 2015, p. 66.

45 Goodman, 'Cyber deterrence: tougher in theory than in practise', p. 117.

46 Lupovici, 'Cyber warfare and deterrence: trends and challenges in research', p. 54.

47 Angela McKay, Jan Neutze, Paul Nicholas, Kevin Sullivan, *International cybersecurity norms: reducing conflict in an internet-dependent worl*d, Microsoft, 2015, p. 9.

48 UN, *Developments in the field of information and telecommunications in the context of international security: report of the Secretary-General*, A/70/172, 22 July 2015, online.

49 The White House Office of the Press Secretary, 'Fact Sheet: President Xi Jinping's State Visit to the United States', 25 September 2015, online.

50 McKay, Neutze, Nicholas, Sullivan, *International cybersecurity norms: reducing conflict in an internet-dependent world*.

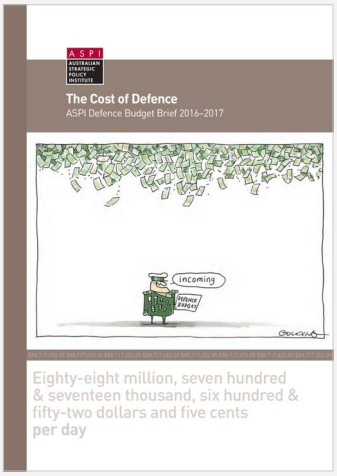
51 Tobias Feakin, Jessica Woodall, 'Cyber confidence building in the Asia Pacific: three big take-aways from the ARF', *The Strategist*, 9 April 2014, online.

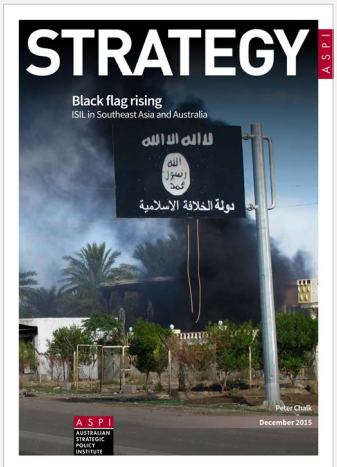
52 Greg Austin, *Australia rearmed! Future needs for cyber enabled warfare*, discussion paper no. 1, Australian Cyber Security Centre and UNSW Canberra, January 2016, p. 12.

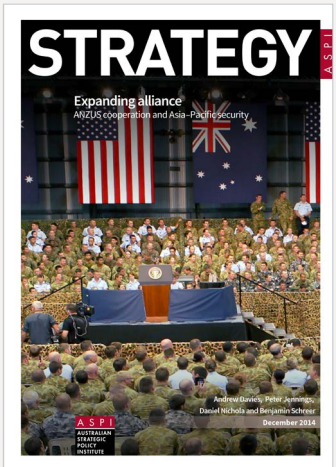
ACRONYMS AND ABBREVIATIONS

ASEAN	Association of Southeast Asian Nations
DoD	Department of Defense (US)
UNGGE	UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
VNSA	violent non-state actor

Some previous ASPI publications







Deterrence in cyberspace

Different domain, different rules

ISSN 2200-6648