Norwegian Institute of International Affairs

Policy Brief
[5 / 2017]

Upholding the NATO cyber pledge

Cyber Deterrence and Resilience: Dilemmas in NATO defence and security politics

Lilly Pijnenburg Muller and Dr Tim Stevens

A secure cyberspace is crucial for the functioning of all NATO member countries in an 'information age' characterized by ubiquitous digital technologies. Our dependence on information technologies has resulted in new and hitherto unknown vulnerabilities being exploited by state and non-state actors on a daily basis. Offensive cyber operations are conducted not only for criminal or commercial gain, but have become an influential factor in international politics. The growing appeal of cyber operations to states and non-state political actors has seen their scale and sophistication increase, showing that cyberspace is becoming normalized as a global environment of competition. States and non-state actors contest cyberspace in pursuit of power and influence. Whilst it might be argued that the effects of cyber operations – subversion, sabotage, manipulation, theft, disinformation – are nothing new, the speed and volume of their deployment are unprecedented. Considerations of cybersecurity are therefore deeply intertwined with all 21st-century political and military conflict. As stated by NATO Secretary General Jens Stoltenberg, 'most conflicts and crises these days have a cyber dimension', and it is 'very hard to imagine a military conflict today without a cyber dimension.'

To ensure NATO keeps pace with the dynamic landscape of cyber threats, the NATO member-states in 2016 signed the NATO Cyber Defence Pledge. In this expression of mutual defence and Allied solidarity, the member-states reaffirmed their commitment to 'enhance the cyber defences of national infrastructures and networks' by developing 'the fullest range of capabilities' to defend them. This document is framed principally in terms of defence and resilience – the ability to 'bounce back' from offensive cyber operations and to maintain operational functionality. There is no mention of 'deterrence' in the Pledge but it is this concept – one that characterises most of Cold War and general defence thinking – that has resurfaced in subsequent NATO discussions about how to uphold the Pledge.

This NUPI Policy Brief clarifies the key concepts of traditional deterrence and then explores how these apply to cyber deterrence. It identifies a range of problems inherent to cyberspace itself and to the translation of existing deterrence models to this domain. It proposes a range of alternative and complementary approaches to deterrence that can assist in developing a new framework for conceptualizing NATO Alliance cyber deterrence. These will all require rethinking cyber deterrence as a condition of success or failure: cyber deterrence must be reframed as an ongoing process, utilizing national and Alliance resources from multiple domains as a means to establish deterrence and resilience.

The concept of deterrence

'Deterrence is the art of producing in the mind of the enemy [...] the fear to attack.' It is the ability to create a perception in the mind of adversaries that you have the capacity to impose upon them significant costs or to limit their possible gains, should they undertake offensive action against you. Deterrence is an inherently coercive component of strategy that involves 'the potential or actual application of force to influence the action of a voluntary agent.' Unlike its coercive twin, compellence, which seeks to alter the course of action upon which an actor has already embarked, deterrence seeks to dissuade the actor from pursuing that behaviour in the first place. It does so by altering the actor's cost-benefit assessments of the various strategic choices available. If an actor perceives that the expected utility of a given action is outweighed by the likely costs, it will be deterred from behaving in that fashion, thereby preserving the status quo.

Deterrence is contingent upon whether an adversary per-

ceives a threat as credible and thus the threats made against it should be considered a psychological issue, not a technical one. This psychological aspect is illustrated by considering the difference between two types of deterrence: deterrence-by-punishment and deterrence-by-denial. Deterrence-by-punishment relies upon the credible threat that overwhelming retaliation will be meted out against an adversary should it attack. Deterrence-by-denial hinges on the defender's ability to deny an attacker's desired ends. The former is purely coercive, whilst denial also incorporates elements of control. Denial in this sense aims to control a situation sufficiently that the opponent is denied certain strategic options, rather than being coerced towards particular behaviours.

Deterrence-by-punishment:
The credible threat that overwhelming retaliation will be meted out against an adversary should it attack.

Deterrence-by-denial:
The defender's ability to deny an attacker's desired ends. It aims to control a situation sufficiently that the opponent is denied certain strategic options, rather than being coerced towards particular behaviours.

As a model of strategic interaction deterrence was deemed successful during the Cold War, as the superpower relationship predicated on nuclear deterrence never entered a nuclear warfighting phase, despite periods of strategic tension and escalation. The apparent success of nuclear mutual deterrence has come to shape subsequent debates about the nature of deterrence and its applicability to other strategic domains. However, the offence-dominance of nuclear weapons is not replicated in environments like cyberspace, nor indeed when conventional weapons are involved. For instance, deterrence-by-denial may occasionally require the demonstration of conventional offensive capabilities to dissuade an attacker – surely not an option with nuclear weapons. The simplicity of nuclear deterrence is also sharply at odds with the complexity of other forms of deterrence, where myriad actors, intentions and technological capabilities co-exist in a matrix of competing forces and possibilities. Therefore, a viable model of cyber deterrence cannot be derived directly from nuclear deterrence theory and practice, although Cold War history may continue to provide useful insights into strategic state-level interactions.

Moreover, it is unlikely that cyber deterrence can prevent all attacks by cyber means. Instead of conflict prevention in line with the nuclear deterrence model, any cyber deterrence posture must seek to shape the conflict space, rather than expecting to dominate it entirely. Many, perhaps even most, offensive cyber operations are not high-level national security threats, but may often be better characterized as criminal actions which require inter-agency and public-private responses, frequently of a non-military and transnational character. Like other forms of crime, these are difficult to deter, and states do so imperfectly. This is not to draw a distinct line between criminal and strategic cyberattacks where one does not exist, but it does recommend clarity in identifying what actions and processes constitute national security threats and which do not. This has significant implications for managing expectations and for resource allocation and, therefore, for how the efficacy of cyber deterrence should be assessed. Any cyber deterrence posture should be underwritten by the understanding that the cyberspace environment is one of 'offence-persistence'. Attacks are frequent, numerous, ongoing, ambiguous and evolving. Cyber conflict is in other words the 'new normalcy' in cyberspace. Yet, strategic cyberattacks are far more difficult to prosecute than is commonly imagined, with the majority of cyber operations being low-level, tactical or criminal.

Attribution and resilience

Cyber deterrence has been the object of substantial military, policy and academic literature. Proposals for cyber deterrence regimes are beginning to crystallise around a set of key operational concepts and considerations. Most practitioners and scholars point to the 'attribution problem' as a key burden in cyber deterrence, arguing that challengers can disguise themselves and thereby obscure the sources of attack, meaning that defenders must invest great forensic efforts to discover them. It has long been recognised by NATO allies that, in order for cyber deterrence-by-punishment to be effective, this potential lack of a 'return address' confounds the ability to demonstrate a credible deterrence posture.

Given this potential obstacle, and the persistence of offensive cyber operations, recent discussions and NATO documents argue for a new deterrence posture better aligned with deterrence-by-denial than with deterrence by punishment. This would aim to diminish the damage and disruption intended by adversaries and reduce their incentive to attack. Knowing we will be attacked, the idea is that the most important action is to build resilience, the ability to perform critical functions regardless of attacks launched. Success in this field would be underpinned by strong proactive and reactive defensive capabilities. Within NATO, this idea of resilience is increasingly seen as the corollary of deterrence and reassurance, and as part of a comprehensive security strategy for the Alliance. However, how such resilience would work, and what this means for deterrence, is unclear.

While attribution certainly complicates the ability to present a credible cyber deterrent, anonymity is not a priori characteristic of cyberspace. Moreover, attribution problems do not necessarily prevent deterrence success. While it can be difficult to trace the source of a cyberattack, the attribution problem is not unique to the cyber domain. Armed attacks, for instance, are often carried out anonymously. Forensic analyses might take time – although investigation cycles

are accelerating with the involvement of private companies in attribution activities – but there are other ways of circumventing the supposed attribution problem.

Attribution is contextual and should not rely solely on technical considerations. Indeed, 'attribution is a matter of interpretation.' It is a political challenge as much as a technical one; very often there are solid reasons for seeing a given actor as involved in a cyber operation, even in the absence of evidence that would meet some putative legal standard. This was clearly demonstrated in Congressional hearings on alleged Russian interference in the 2016 US presidential elections. When asked whether they believed that Russia was behind these operations, even in the absence of a 'smoking gun', all witnesses testified 'yes.' This conclusion was reached by considering a range of political, technical and strategic factors, all and any of which may change over time.

The 'attribution problem' may therefore not represent such an encumbrance to deterrence as is commonly supposed, and we should not exclude traditional notions of deterrence-by-punishment from present considerations. However, some further comments are necessary on specific conceptualizations of deterrence that may have applications in the cyber domain.

Reconsidering deterrence

Trans-event deterrence
In an offence-persistent environment, deterrence cannot be situated purely with reference to discrete events, like pre- or post-event deterrence actions. Nuclear deterrence and many aspects of conventional deterrence are contingent on singular events, usually acts of war or combat strikes that are uniquely located in space and time. This cannot be the case with cyber deterrence, where we must think in terms of ongoing processes instead of events, and which are distributed in time and space. Traditional notions of territoriality and temporality are not always applicable in the cyber domain. This means that cyber deterrence must also be identified in its trans-event dimension, in addition to its pre- and post-event aspects.

Deterrence by entanglement
Sometimes called 'self-deterrence', deterrence by entanglement refers to the existence of various interdependencies that result in a successful attack simultaneously imposing serious costs on the attacker and the victim. This line of thinking regards cyberspace as a global commons – which would mean that all states have an interest in reaping its benefits and will restrain their actions accordingly. There is today no formal acceptance that cyberspace is such a global commons, which militates against the entanglement argument in some respects. However, the interconnectedness of cyberspace and the potential for cascading effects and unforeseen outcomes in the form of 'blowback' must be considered by any attacker, particularly those dependent on highly developed information infrastructures.

Norms-based deterrence
As with nuclear weapons, it is not only the weapon that needs to be understood but also those who have access to these weapons. Deterrence becomes a question not only of technical capability to act but also of an actor's motives and intentions to act, and the social, cultural and political factors that shape them. From a norms-based perspective, deterrence is a consequence, inter alia, of political considerations like the value of the target and the scale-dependent cost of exploitation and retaliation. The failure to employ cyber deterrence successfully is not determined by the technical challenges of cyberspace, but by how the effects of these challenges are mediated through social context(s) and norms. However, the utility of norm-based deterrence against non-state actors is limited, where the ability to communicate norms becomes restricted and normative reciprocity cannot be expected.

Cumulative deterrence
The cumulative deterrence paradigm does not unrealistically seek to prevent cyberattacks from ever occurring. Instead, it takes for granted the inevitability of acts of cyber aggression and strives to shape and limit them by attacking the rival repeatedly in response to specific behaviours over a long period, sometimes even disproportionally to its actions. Restrictive in nature rather than absolute, it perceives deterrence as a spectrum, not a dichotomous, binary state. It is concerned with degrees of deterrence, instead of simply assuming its total presence or absence. Importantly, it is inherently cross-domain, in that deterrence activities are not to be restricted to cyberspace alone: they must also involve kinetic operations, in addition to the levers of diplomatic and political influence. This framework also incorporates aspects of compellence, because it seeks not only to deter adversarial behaviours but to shape those already in play.

Conclusions
This policy brief has drawn attention to the need to reconceptualize NATO's cyber deterrence thinking and posture. Traditional models of deterrence, drawn from the nuclear and conventional deterrence thinking of many decades' standing, are inadequate for addressing the challenge of deterring cyber threats in the 21st century. The dynamism of the environment, the range of threats, the multiplicity of state and non-state actors, and the technical challenges of attribution – all require a reorientation of deterrence posture and practice. This reconceptualization must focus on cyberspace itself in an intensification of attention to its idiosyncrasies, but should also be open to a relaxation of orthodoxy in its incorporation of new outlooks and ideas, some of which may strain the established boundaries of deterrence theory.

A future NATO cyber deterrence regime will need to look

beyond the military aspect and consider the context of adversarial decision-making in its social and political dimensions. It must also connect cyberspace operations with those in other domains of national and NATO power in a deliberately cross-domain framework. Deterrence should be understood as a cumulative process of ongoing offensive and defensive operations that repeatedly demonstrate intent and capability as a means of generating credibility. This includes elements of compellence, as well as deterrence. Deterrence and resilience should be seen as integral components of this process, with significant overlap between each. Indeed, resilience can work as a form of post-event deterrence-by-denial, which, if successful, may reduce adversaries' cost-benefit analyses. Such a new framework for cyber deterrence will accept that cyberattacks will happen, recognizing that this is not necessarily a 'deterrence failure' but may represent an opportunity to learn and adapt.

A renewed commitment to cyber deterrence and resilience will help to uphold the NATO Cyber Defence Pledge, but it will require revising our conventional models. Deterrence must be rethought, from a Cold War relic to a modern, flexible and dynamic process of national and Alliance operations. Cyber deterrence is not a static binary state of success or failure – it involves a whole range of possibilities for shaping the conflict environment. In this policy brief, we have indicated some avenues for exploration and conceptual development.

Note

This Policy Brief has also been published with full references on:
http://www.nupi.no/en/About-NUPI/Projects-centres-and-programmes/Cyber-Security-Centre/Upholding-the-NATO-cyber-pledge

Norwegian Institute of International Affairs

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from short-term applied research to more long-term basic research.

About the authors:

Lilly Pijnenburg Muller is a Research Fellow in the Research Group for Security and defence at the Norwegian Institute of International Affairs (NUPI) with a focus on cybersecurity. Within cybersecurity her research covers public-private cooperation, multi-stakeholder processes, capacity building in developing countries, risk and harm. In addition, she follows international cybersecurity processes in the UN, OSCE and NATO. Previously she worked as a James Martin Fellow at the University of Oxford at the Martin Schools Global Cyber Security Capacity Building Center (GCSCC).

Dr Tim Stevens is Lecturer in Global Security in the Department of War Studies, King's College London. His research engages with political and strategic aspects of cybersecurity and cyberwar and has been published widely, including Cyber Security and the Politics of Time (Cambridge University Press, 2016). Other relevant and recognized publications include "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace", Contemporary Security Policy, 2012, and Cyberspace and the State: Towards a Strategy of Cyber-Power (Routledge, 2011).

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
PO Box 8159 Dep. NO-0033 Oslo, Norway
www.nupi.no | info@nupi.no