CHACR Global Analysis Programme Briefing

IN DEPTH

CHACR

ISSUE 16 , FEBRUARY 2019

Re-Thinking Deterrence

Image Source: Bournemouth University

Executive Summary

Deterrence by punishment has served Western countries well. With the exception of a small number of cases, since the end of World War II Western allies – whether acting in informal alliances or as NATO – have been able to stave off armed attacks on their territories and armed forces. The emergence of international terrorist organizations with nation-state ambitions began to pose additional challenges on traditional deterrence. Now nation states' changing behaviour is posing far more fundamental challenges. Countries such as Russia and China could dramatically destabilise target countries by exclusively using non-military aggression. As the current extent of the activities is already proving, deterrence by military punishment is of limited effect. While societal resilience is not a new concept or practice, today it is severely underutilised. Since hybrid/greyzone/threshold warfare uses seamless aggression, only seamless – combined – deterrence can be effective against it. Working with industry and the wider population, Western governments should enhance societal resilience and use it to strengthen existing deterrence.

ABOUT THE AUTHOR

Elisabeth Braw

Elisabeth Braw is an Associate Fellow at RUSI and Director of RUSI's Modern Deterrence Programme.

Note:

The views expressed in this In Depth briefing are those of the author, and **not of the CHACR or wider British Army**. The aim of the briefing is to provide a neutral platform for external researchers and experts to offer their views on critical issues.

Centre for Historical Analysis and Conflict Research
Robertson House, Slim Road, Camberley
GU15 4NP
Telephone: 01276 412708 Mil: 94261 2708
Facsimile 01276 412708 Mil 94261 2708

Background: What is Deterrence?

What is deterrence? Given that Western countries have been focusing on deterrence as a priority since the end of World War II, the question may seem frivolous. Nevertheless, with aggression against Western countries on the increase, the question must be asked. As Mazarr et al note, "perhaps the narrowest definition, but also one of the most common, holds that deterrence refers to the strategy of using the threat of military response to prevent a state from taking an action it feels tempted to take"[1]. Peter Roberts and Andrew Hardie list four criteria for successful deterrence:

"For state A to successfully deter state B, state B MUST know that state A has the following:

1. The capabilities required to harm state B.
2. The will to launch a credible reprisal and the reputation that it would.
3. Knowledge of what will cause state B such losses as to deter it in the first place.
4. The resolve to accept any harm to it that may be caused by a reprisal act in response to the original the deterrent act."[2]

Edward Luttwak, in turn, summarises deterrence as military inducement, which he divides into latent inducement (inherent deterrence and precautionary posture) and active inducement (supportive action and military coercion, with the latter divided into compellence and active deterrence). As Michael Codner notes, "the factors essential to understanding inducement are generally that effect is achieved through influencing the **perceptions** of actors—whether these are actual or potential opponents, actual or potential friends, or the wide number of different stakeholders for whom the consequences may be a mere spectrum of engagement from consent through to assent to mere acquiescence."[3]

The consensus has been that during the Cold War, thus defined deterrence was by and large successful in preventing armed conflict between NATO and the Warsaw Pact. The end of the Cold War and the emergence of global terrorism prompted a change of approach that ultimately yielded limited success, as terrorist networks and lone-wolf terrorists operate differently than rational state actors. Today it is evident that nation states still need to be deterred. Russia's 2014 annexation of Crimea and incursion into eastern Ukraine is evidence of the need for renewed nation-state deterrence, as is China's incremental construction of artificial islands, and maritime policing of them, in a strategic and disputed part of the South China Sea. The deterrence definitions of Mazarr et al and Hardie and Roberts still apply to such military-based aggression.

The resurfacing assertiveness does, however, not stop at military actions. Russian hacker groups operating as government proxies have, for example, directed viruses at Ukrainian institutions. In 2015 and 2016, an attacker – later identified as the Kremlin-linked hacker group Sandworm -- infected Ukrainian utilities with malware, an act that left hundreds of thousands of Ukrainians without power.[4] The 2017 NotPetya virus, subsequently likewise traced to Sandworm, hit Ukrainian institutions and companies and travelled on to international targets. The Danish shipping giant Maersk's IT system was rendered virtually useless for a week, causing Maersk an estimated $300 million in losses. FedEx was likewise hit, as were the pharmaceutical company Merck and the National Health Service in the UK.[5] Russian news outlets, for their part, transmit disinformation about Western countries at high speed and in large quantities. Among examples from January 2019: Sputnik's German edition reported that the Former Yugoslav Republic of Macedonia was being forced by NATO to change its name.[6] Russian Channel 5 TV claimed that Lithuanian WWII freedom fighters had killed Lithuanian women and children.[7]

Chinese companies linked to the government, meanwhile, have been buying critical national infrastructure assets and strategic companies in Western countries. In recent months, three pioneering Swedish semiconductor companies that also supply technology to the Swedish armed forces have been acquired by Chinese companies.[8] Citing national security concerns, Australia and New Zealand have banned the Chinese telecoms giant Huawei from providing 5G technology; the Unites States and other countries have similar concerns. In Denmark, the government has been forced to buy back a former naval base from the private owner in order to prevent a Chinese acquisition. Unlike computer attacks and disinformation, acquisition of strategic assets is legal.

Both approaches, though, present Western allies with a conundrum. The threat of military response clearly does not deter non-military attacks on civil society. In addition, attacks below the Article 5 threshold create confusion as to whether nation-state aggression is taking place. "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them […] will assist the Party or Parties so attacked," states Article 5 of the Washington Treaty.[9] Even under a liberal interpretation of the term armed attack, disinformation campaigns and computer viruses directed at railways or shipping companies do not constitute an armed attack. Neither does the gradual construction of artificial islands in disputed waters. Salami-sliced aggression thus evades traditional deterrence by punishment. In addition, as Mazarr et al point out, "trying to respond to everything can 'cheapen the currency'".[10]

As a result, the wider Western defence community even disagrees about the Western alliance is at currently war with Russia, China and/or other state actors. It is, however, beyond dispute that certain nation states – and groups affiliated with them – are subjecting Western countries to aggression below the Article 5 threshold with the objective of weakening them. Oona Hathaway and Scott Shapiro have documented how territorial conquests have gradually declined; Russia's annexation of Crimea constituted an exception to this trend.[11] That does, of course, not mean that countries should dismantle their military defence. It does, however, constitute hybrid/greyzone/threshold warfare with a growing emphasis on non-military aggression.

Maj Gen Gunnar Karlson, the director of Sweden's military intelligence and security agency (MUST), characterises such aggression as having the aim to "steal, disrupt and destroy".[12] Unlike traditional warfare, which targets enemy forces and their supporting infrastructure, hybrid warfare's strong non-kinetic opponents target civil society. Such attacks, for example on the power grid or the internet, can critically disrupt daily life in the targeted country. Any extended power or internet outage would, in addition, have substantial cumulative effects across all the areas included in NATO's resilience baseline requirements. These are:

- assured continuity of government and critical government services
- resilient energy supplies
- ability to deal effectively with the uncontrolled movement of people
- resilient food and water resources
- ability to deal with mass casualties
- resilient communications systems; and finally
- resilient transportation systems

Indeed, sub-Article 5 attacks could cause as significant damage to the targeted country as a military attack. In addition, aggression by means of malign influence can cause substantial damage to societal cohesion and popular trust in a country's institution. Such damage remains far longer, and is harder to repair, than physical damage.

Designing A New Model of Deterrence

Given these changing characteristics of aggression directed towards them, it is imperative for Western allies to update deterrence. Without doing so, they risk exacerbating a situation where their traditional, armed forces-focused deterrence remains effective, but adversaries increase their focus on sub-Article 5 aggression against softer targets.

Deterrence can be viewed as a pyramid. At the top is the nuclear deterrent, followed -- at the next level down -- by deterrence by punishment (executed through armed forces). Below deterrence by punishment resides deterrence by denial, typically thought of as traditional defence and sometimes political means such as sanctions. Deterrence by denial, though, needs to contain a much stronger societal resilience component.

Deterrence by denial must instead incorporate the civilian population in their everyday lives. While the armed forces and political decisions may fail to deter sub-Article 5 aggression, deterrence by denial could – with the addition of societal resilience -- play a key part, simply by minimising the impact of any attack and thus changing the aggressor's cost-benefit calculations.

With the incorporation and expansion of existing societal resilience, deterrence by denial thus forms a fundamental level of deterrence. The addition of societal resilience reduces the aggressor's benefits from such activities. At Sweden's 2019 Folk och Försvar defence conference, a mayor whose city council is working with the Swedish armed forces to establish comprehensive defence in her community labelled the deterrence responsibilities of civil society thus: "Attacking us has to be like pouring water on a duck's back." Such comprehensive deterrence means shifting deterrence from a passive posture to a dynamic state of mind that reaches across society. With everybody potentially targeted by aggression, everyone has a role to play in deterring it. Rather than having the armed forces and the government act as a shield for the rest of society, the collective society forms a combined shield.

For most countries, such an approach and practice would constitute a significant shift. Since the end of World War II, most mature democracies have opted to entrust national security almost exclusively to government-led institutions (including the armed forces). While most Western European countries – with the notable exception of the United Kingdom – maintained conscription until the first decade of this century, most countries gradually decreased the number of conscripts until the draft was suspended.[13] Though general conscription for men – and it could be argued that today women, too, should be included in any conscription legislation – contributes to deterrence by increasing a country's military manpower and signalling comprehensive resolve, larger numbers of soldiers would in most cases not solve the dilemma of how to deter non-military attacks. In should also be remembered that conscription armies require large manpower resources for training of conscripts—a daunting challenge for today's armed forces, most of which struggle to recruit and retain personnel.

During World War II and the Cold War, Sweden pioneered this approach as a response to the overwhelming power of its adversaries, Nazi Germany and the Soviet Union, respectively. The Swedish model – labelled Total Defence and subsequently adapted, to different extents, by Finland, Denmark and Norway – takes a whole-of-society approach to defence, with every able-bodied and able-minded adult having a role to play in national defence. During the Cold War, that role could be as small as knowing what to do in case of a nation-wide radio alert, or seconding one's tractor to the government for war duties or exercises.

After the end of the Cold War, Sweden largely dismantled Total Defence; to a lesser extent, so did Norway and Denmark. Total Defence's population-centric approach can, however, be used as a basis for comprehensive deterrence against hybrid/greyzone/threshold warfare. Indeed, most developed countries could benefit from using the pillars of Total Defence as the foundation for modern deterrence.

Today there is clearly little need to lend the government tractors. There is, however, still a need for wider populations to know how to fend for themselves in case of a crisis, whether that crisis be a military attack or – more likely – a sub-Article 5 attack. That is even more true as attacks on the technology that forms the basis of 21st-century daily life constitute a highly effective form of hybrid warfare. Though legal, un-transparent takeovers of Western cutting-edge technology firms or other strategic assets must therefore be considered part of hybrid warfare.

Given that the aim of the West's adversaries is to "steal, disrupt and destroy", it is logical the Swedish Civil Contingencies Agency's *If War or Crisis Comes* brochure, sent by post to every Swedish household in May 2018, advises residents on how to go about daily life in case of disruption of power or the internet. While public authorities are responsible for the country's safety, the brochure explains, "everyone who lives in Sweden shares a collective responsibility for our country's security and safety. When we are under threat, our willingness to help each other is one of our most important assets."[14] The brochure also teaches residents how to identify disinformation—a crucial aspect, given that disinformation can seriously destabilise the country targeted by it.

Involving civil society in defence and deterrence raises considerable additional considerations. How, for example, can private companies in strategic sectors best cooperate with the government for the sake of national security? Cabinet-level crisis management exercises involving both cabinet ministers and CEOs have long been a stated objective of many governments. Such exercises should be implemented and conducted regularly. Not least since the Maersk incident, business leaders have realised that they are part of national security and that it is in their interest to maintain seamless crisis management cooperation with the government. Government-industry cooperation in punishment of IT aggression – whether open or clandestine – should likewise be considered, as united defence against such aggression would strengthen deterrence.

A more challenging aspect is how to incentivise companies to have backup plans in case of disruptions resulting from hostile attacks. Unlike the Cold War years, today critical national infrastructure is largely owned by private companies rather than the government. Given the widespread chaos that would be likely to result from, for example, a sustained power or internet outage, such backup plans form a vital part of deterrence by resilience. However, since they are more likely not to be attacked than they are not to be attacked, companies – which operate on the basis of quarterly results -- are reluctant to allocate funds to backup plans. They could, for example, be incentivised by tax breaks or by being granted government status as resilient companies. The government could even subsidise backup plans. Through investments and other financial incentives, it could also prevent takeovers by of national companies in strategic sectors by questionable foreign-linked entities. As a last resort, it can legislate resilience requirements. The Swedish government, which is in the process of re-establishing and modernising Total Defence, has appointed a commission to investigate ways in which the private sector can be incentivised to contribute to societal resilience.

The wider population can be similarly incentivised to participation in resilience. Brochures like the MSB's *If War or Crisis Comes* could be distributed in other countries as well; in ones farther from the frontline with Russia, there could be a stronger focus on environmental crises, which similarly cause disruptions to daily life. As earthquake regions – for example San Francisco and Japanese prefectures – illustrate, consistent preparedness education instils confidence among residents, not fear. Governments could also offer citizen resilience training; attendance could be encouraged by granting graduates resilience status or tax breaks. There could also be general resilience training for 18-year-olds; a more effective – and cheaper – option than conscription.

As successful adversaries exploit gaps, modern – comprehensive – deterrence will, however, only be effective if its segments are closely connected. With the government acting as the facilitator of comprehensive deterrence rather than sole provider of it, the armed forces, other parts of the government, the private sector and wider population will thus need to constantly plan and exercise their cooperation. Though unwieldy, only regular general exercises would create the desired efficiency. Switzerland's nation-wide Sicherheitsverbundsübung is an exemplary model of comprehensive practice. The first Sicherheitsverbundsübung, involving participants from government, the private sector and the wider population, took place in 2014. The next one will take place in November 2019, focussing on a simultaneous national power outage and influenza pandemic.[15]

Countries should conduct such exercises in a public manner, as it would reassure the public and allies. More importantly, such public exercising brings significant stratcom value. In other words, such displays of national unity influences opponents' perceptions of Western strength. That strengthens deterrence.

Conclusion

Deterrence theory rests on the assumption that adversaries are rational actors. Today's hybrid/grey zone/threshold warfare illustrates that very rationality. Sensing little opportunity in military aggression, the West's adversaries – currently primarily Russia, as well as China -- are maintaining their military capabilities. That ensures that mutual deterrence by punishment remains in place. At the same time, they are refocusing their power-gain efforts on segments with more potential, that is: civil society. As deterrence is only as strong as its weakest link, societal resilience thus represents a significant liability. Western countries must change adversaries' cost-benefit calculations by strengthening deterrence by resilience and thus deterrence by denial. If government-led deterrence by punishment fails – as is typically the case with sub-Article 5 aggression -- an engaged and trained civil society can act as an additional deterrent by altering the would-be-aggressor's cost-benefit calculation.

End Notes

1. Michael J. Mazarr, Arthur Chan, Alyssa Demus, Bryan Frederick, Alireza Nader, Stephanie Pezard, Julia A. Thompson, Elina Treyger: What Deters and Why. Exploring Requirements for Effective Deterrence of Interstate Aggression. 2018: RAND Corporation, p 3.
2. Peter Roberts and Andrew Hardie: Is deterrence a valid philosophical concept for the next twenty years? RUSI Occasional Paper
3. Anthony Cain (ed): Deterrence in the twenty-first century. London 2010: RUSI, Air Force Research Institute and King's College London, p 19
4. *Wired,* 7 December 2017, https://www.wired.com/story/russian-hacking-teams-infrastructure/
5. *Wired,* 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
6. European External Action Service East Stratcom Task Force, https://euvsdisinfo.eu/report/macedonia-is-forced-by-foreign-countries-to-access-nato-and-change-its-name/
7. https://www.5-tv.ru/glavnoe/broadcasts/509872/1183/
8. Birgitta Forsberg, Statliga Rymdbolaget skrev avtal med kinesisk militär, *Svenska Dagbladet*, 18 January 2019, https://www.svd.se/staten-salde-spjutspetsbolag-till-kina--trots-militara-kopplingar
9. NATO: The North Atlantic Treaty, https://www.nato.int/cps/ie/natohq/official_texts_17120.htm
10. Mazarr et al, p 31
11. Oona Hathaway and Scott Shapiro: *The Internationalists.* New York: Simon & Schuster (2018)
12. *Dagens Industri,* 20 January 2019; https://www.di.se/nyheter/mustchef-sakerhetshotet-mot-sverige-ar-allvarligt/
13. Lithuania has since introduced selective conscription, as has Sweden.
14. Swedish Civil Contingencies Agency: *If War or Crisis Comes.*, 2018. https://www.msb.se/Upload/Forebyggande/Krisberedskap/Krisberedskapsveckan/Fakta%20om%20broschyren%20Om%20krisen%20eller%20Kriget%20kommer/If%20crises%20or%20war%20comes.pdf, p 3
15. https://www.vbs.admin.ch/de/themen/sicherheitspolitik/sicherheitsverbundsuebung-2019.html