Societal Resilience as a Deterrent

Elisabeth Braw and Peter Roberts
61 Whitehall
London SW1A 2ET
UNITED KINGDOM

elisabethb@rusi.org

ABSTRACT

The primary concern of every government is the well-being of its population. As the threats to western countries' national security increase and intensify it is becoming clear that governments and their armed forces alone do not have the capacity to provide sufficient protection and mitigation in every area of society. This is especially important to consider as threshold or hybrid warfare and other emerging forms of war increasingly target Western countries' soft underbelly: their civil societies and private sectors. To a large extent, such aggression is not impeded by geography: cyber attacks and malign influence campaigns know no geographical impediments, but they can cause harm to the homeland that is as effective as military aggression.

In addition, today many of the targets of potential aggression – for example companies in strategic sectors – are owned not by the government but by private shareholders, nor are they classified as critical national infrastructure that qualifies for additional protective measures.

This means that governments need to work with business to create a model of comprehensive resilience and thus deterrence. Indeed, governments need to re-evaluate their approach to societies' involvement in these challenges. That is all the more important as societal resilience can act as a deterrent. Several countries have shown that it is possible and desirable to involve citizens in some form of an organised homeland defence. Denmark's volunteer Home Guard frees up the armed forces to focus on purely military duties. The Swedish government has been updating its Cold War total defence plans, where the population play a major role. In a crisis situation, residents of Sweden are now expected to be able to support themselves for seven days. Ahead of the September 2018, Swedish national elections, the Swedish Contingencies Agency (MSB) trained civil servants and the wider public how to identify Russian interference attempts. With the population thus prepared, the cost/benefit calculus of an adversary changes.

No country, however, has comprehensive societal resilience plans. With most developed countries facing hybrid threats of a similar nature, there is opportunity - and a need - to build on current models. Philosophically this is a challenging move for governments: it shifts an underpinning belief in deterrence as a passive, dormant posture to which governments are solely responsible, to an active and dynamic state of mind that reaches across society, where everyone plays a part. With our population and private sector, however, our societies harbour enormous deterrent potential.

1.0 BACKGROUND: THE NEED FOR SOCIETAL RESILIENCE AS A DETERRENT

The primary concern of every government is the well-being of its population. The United Kingdom's 2015 National Security Strategy and Strategic Defence and Security Review, for example, lists as National Security Objective 1: "To protect our people – at home, in our Overseas Territories and abroad, and to protect our territory, economic security, infrastructure and way of life."[1] For the past several decades, most developed countries have taken a similar approach, viewing their populations as entities that needed protection from war, natural disasters and other calamities. Indeed, the majority of residents in most developed countries – even those with national service – are never asked to perform any duties in the service of national security. In times of peace, that is a workable model. We are, however, living in an age multiplying, and evolving, threats that extend beyond conventional military actions. That raises new questions about how our societies should protect themselves and deter aggression.

The central consideration in such a query is the adversary's perspective. What matters is not simply the adversary's aims and the objectives the adversary calculates the destabilising activity will achieve, but in the adversary's own cost-benefit analysis: Are the gains from such actions worth the costs of undertaking them? By understanding this equation for an adversary or competitor, one can better adapt models of deterrence and resilience to ensure they have the desired impact.

Rivals' cost-benefit equation

Whilst such calculations are worthy of undertaking for all adversaries, and acknowledging that each of these entities will have contextually different costs and benefits, it is worth understanding a state actor as an initial example. The principles and processes that emerge from such an examination can be extrapolated and applied to other adversaries, competitors and actors.

For much of Western Europe, the primary state protagonist might be considered to be Russia. Whether challenging the rise of democratic values in Georgia and Ukraine through military action, or undertaking subversive actions against European societies across the continent, Russia has been instrumental in undermining many of the core principles of European state identity and philosophy. Moscow challenges the ideology of liberal democracy through subversion, espionage and sabotage. Most of the time, these undertakings carry only minor financial costs. The cost of cyber-attacks, for example, is negligible. Other activities burn greater capital – but rarely financial. The consequences of the Russian nerve agent attack in Salisbury, UK was high in diplomatic terms: the expulsion of 69 Russian officials from Europe and the United States placed Russia in a more precarious position than it had previously been in terms of the presence of officials in foreign states. In other ways, however, Russia lost very little by conducting the attack. Even if the deployment and use of a nerve agent in a NATO state had not been approved by the highest levels in the state, there is some doubt whether it would have been vetoed had it been put to President Vladimir Putin himself.

This is useful to consider: actions by Moscow are not simply weighed in purely financial terms. Rather they are measure for the benefit they bring. For Russia, the benefit might be better understood in terms of public opinion, not political legitimacy or monetary cost.

Given this reality, deterring hostile actions by increasing the cost is more difficult. A more promising approach for the West to take might instead be to reduce Russia's benefits from such activities. Such an action is, however, at odds with much of modern (post-Cold War) thinking on deterrence, which actively

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/555607/2015_Strategic_Defence_and_Security_Review.pdf

models deterrence in financial cost terms.[2] Similarly, deterrence by punishment looks less likely to provide useful results when the actions that one party is attempting to deter fall below the threshold of a military response.[3] Such conclusions are not necessarily new.

In their scholarly review of academic literature surrounding deterrence, Zagare and Kilgour concluded that deterrence is a tenuous, fragile and unstable interaction where conflict is always possible.[4] It seems as though deterrence consistently fails, according to the literature at least, and that the theoretical frameworks are too simplistic to prove utility. Zagare and Kilgour conclude: "It should not be considered a reliable tool for statecraft".[5] They are not alone in their evaluation. Lebow and Stein found in their studies that deterrence rarely works, but that it has become such commonplace language in policy discussions that leaders can find themselves in a "Deterrence Trap", in which policy makers faced with a challenge will not find a 'good' outcome and will thus be forced into selecting from between appeasement or retaliation.[6]

Classical deterrence theory has existed in many forms since considerations about the phenomena were explored by Thucydides, who framed the deterrence and compellence as a strategic interaction problem. His findings, according to Richard Lebow, emphasise the determining importance of motives for the strategic calculus of actors. It is also noteworthy that Thucydides concluded that deterrence strategies usually failed and tended to help provoke the behaviour they were intended to prevent. The targets of deterrence tended to downplay risks and costs when it was contrary to their desires or needs.[7]

Conversely, many authors have found both utility and validity in deterrence as both a state of mind and a strategic option. Lawrence Freedman's study of the subject was clear in that policy makers understood the examples rather than the theory, and that away from the scholarly interpretations and inside real examples, deterrence remains as valid as it has historically been.[8] Importantly, Freedman notes that "The starting point is that deterrence does not offer a self-contained strategic relationship but is part of a wider set of relationships."[9]

Given the wide acceptance that times and perspectives have changed in recent years, it is perhaps time that deterrence was re-defined and composed in a way fit for a modern world.

2.0 THE NEED FOR A NEW DETERRENCE MODEL

Increasing geopolitical tensions have, especially during the past four years, manifested themselves in growing military aggression by Russia and China: Russia's war in eastern Ukraine is a notable example, as is China's construction of artificial islands in a strategic part of the South China Sea and subsequent aggressive naval policing of them. Today this kind of military assertiveness is increasingly accompanied by non-military aggression such as cyber attacks and malign influence campaigns. The seamless blend is commonly referred to as hybrid warfare. To be sure, non-military tools used for aggressive geopolitical purposes are not new. During the Cold War, for example, both Western and Warsaw Pact governments funded front

[2] Adam Lowther, *Deterrence: Rising Powers, Rogue Regimes, and Terrorism in the Twenty First Century* (New York: Palgrave MacMillan, 2012), pp.43.

[3] Elli Lieberman, *Reconceptualising Deterrence: Nudging Toward Rationality in the Middle East* (Abingdon, UK: Routledge, 2013), pp.211.

[4] Frank Zagare and Marc Kilgour, *Perfect Deterrence* (Cambridge, UK: Cambridge University Press, 2000).

[5] Ibid, p.4.

[6] Richard Ned Lebow and Janice Gross Stein, "Beyond Deterrence," *Journal of Social Issues* 43:4 (1988), 33–35.

[7] Richard Ned Lebow, "Thucydides and Deterrence", Security Studies, 16:2 (2007), 163-188.

[8] Lawrence Freedman, *Deterrence* (Cambridge, UK: Polity, 2004).

[9] Ibid, p.5.

publications with slanted articles. The rapid advance of technology has, however, created enormous opportunities for far more potent non-military aggression that can, depending on the attacker's preference, be directed at very large numbers of people (a hack of the electricity grid) or at specific individuals (Facebook ads and fake groups).

Non-conventional attacks are not just easy to hide; they can cause enormous damage on the target country. Such non-conventional parts of hybrid warfare typically target a country's companies and civil society, not its armed forces. That is logical, as civil society forms any open society's soft underbelly. Last year Maersk, the Danish shipping company that accounts for 15 percent of global shipping, was attacked by a virus that disabled the company's IT system, causing losses of $300 million.[10] The virus was later identified as NotPetya, which had been created by the GRU-affiliated Russian hacker collective Sandworm and had previously deployed against Ukrainian government agencies and companies.[11] All had seen their operations disrupted by the attack. When the virus hit Maersk, countless Maersk customers were left without their goods. FedEx, for example, lost some $400 million as a result of the attack. The French construction conglomerate Saint-Gobain lost a similar amount; the British manufacturer Reckitt Benckiser lost $129 million, and Cadbury's owner Mondelēz lost $188 million.[12]

As the Maersk case illustrates, attacks on companies in strategic sectors – such as food/water, energy, transport, financial services, sewage – can rapidly cause severe disruptions. Today's threat scenario also extends to North America, whose location means it has historically for the most part been spared from conventional military threats. According to a study by Lloyd's Insurance, an attack on the energy grid covering the North Eastern United States would leave 93 million people without power. It would disrupt water supplies and wreak havoc on transportation.[13] Such disruption is a tangible risk: between 1992 and 2006, Russia imposed at least 55 energy cut-offs in different countries[14].

Or consider food supplies. The United Kingdom, for example, imports 49 percent of its food.[15] As a result of the advance of the so-called just-in-time delivery model, distribution centres keep only minimal stocks. According to statistics from the UK Department for Environment, Food and Rural Affairs, between 2010 and 2015, 52 per cent of suppliers reduced their distribution centre stock levels. Only 22 per cent increased their stock.[16] Figures are similar in other developed economies.

Indeed, because the vital functions of our societies are now so dependent on technology, so interconnected and so dependent on complex supply chains, cyber attacks and other forms of sabotage against infrastructure such as ports, utilities, the mobile network or the grid can quickly grind daily life to a halt. As Sir Toby Harris notes in an article provided to participants at a recent RUSI conference: "In the event of a widespread power outage, for example, many services would simply stop being provided. Unless a hospital has its own emergency generator it will cease to function, and even then it assumes that other utilities would continue to be available and that staff would be able to report for work. In many areas, without power fresh water cannot be guaranteed and waste water and sewage cannot be removed and treated, and those areas would rapidly be rendered uninhabitable. Telephony would fail and so would mobile communications. ATMs and petrol pumps would stop working. Under such circumstances, civil order would probably break down within

[10] https://www.theregister.co.uk/2017/08/16/notpetya_ransomware_attack_cost_us_300m_says_shipping_giant_maersk/

[11] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[12] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[13] https://www.lloyds.com/~/media/files/news-and.../business-blackout20150708.pdf

[14] https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

[15] https://www.gov.uk/government/publications/food-statistics-pocketbook-2017/food-statistics-in-your-pocket-2017-global-and-uk-supply

[16] https://www.gov.uk/government/publications/food-statistics-pocketbook-2017/food-statistics-in-your-pocket-2017-global-and-uk-supply

a very short time." The Developments Concepts and Doctrine Centre (DCDC), the UK Ministry of Defence's think tank, makes a similar point, stressing that "the increasingly interdependent nature of technology and infrastructure creates the potential for complex scenarios that are likely to challenge the capabilities of conventional emergency responders".[17] Today non-conventional attacks are no longer limited to use as an accompaniment to military action: they can, on their own, can visit enormous damage on another country.

For deterrence planning, these threats pose a conundrum. As Peter Roberts and Andrew Hardie note in a RUSI Occasional Paper, "for state A to successfully deter state B, state B MUST know that state A has the following:

1. The capabilities required to harm.
2. The will to launch a credible reprisal and the reputation to do so.
3. Knowledge of what will cause the aggressor such losses as to deter them in the first place.
4. The resolve to accept any harm to it that may come about die to the deterrent act."[18]

As the authors point out, deterrence by punishment works when the adversaries are rational-thinking state actors using armed forces. NATO's Article 5, of course, rests on the concept of deterrence by punishment. Since the end of World War II deterrence by punishment has worked so well that neither of the resulting parties – NATO and the Soviet Union, followed by NATO and Russia, has been subjected to a military attack by the other side.

The challenge, then, is how to deter non-conventional attacks against civil society, actions that are underhanded and for the most part carry no return address. The deterrence by punishment model is plainly of limited use against such threats. Successful though it has been against conventional threats, NATO's Article 5 can only be used against clearly identifiable adversaries. While the targeted entity may succeed in gathering a good understanding of an attack's provenance, the perpetrator usually does not claim responsibility for a hybrid attack. In the case of the virus that struck Maersk, neither Sandworm nor its Kremlin backers claimed responsibility. Even if perpetrators do identify themselves, they may be hacker groups such as Sandworm, with links to state actors virtually impossible to prove beyond doubt. Indeed, though hackers may be operating on behalf of a government, that link is left to the targeted entity to prove.

Furthermore, escalation in the non-conventional domain is far less predictable than in the conventional, military, domain, simply because the aggressor cannot be assumed to be a state acting according to the patterns established by military strategists. The fact that non-conventional acts of aggression can be efficiently used in conjunction with conventional military actions such as missile strikes further muddies the waters.

That is not to say that potential deterrence by punishment of non-conventional aggression should be excluded from consideration. On the contrary, punishment options such as traditional military punishment, should go hand in hand with societal resilience, always with the goal of forming a complete deterrent posture. Countries must make aggression against them as unattractive as possible. In reality, this may mean redirecting an adversary's aggression towards a country equipped with less comprehensive deterrence.

[17] Developments, Concepts and Doctrine Centre (2017): UK Operations: the Defence Contribution to Resilience and Security, p 15

[18] Roberts, Peter and Andrew Hardie: Is deterrence a valid philosophical concept for the next twenty years? RUSI Occasional Paper

One potential avenue of punishment in the cyber sphere is being tested by the United States Cyber Command. According to news media report, US Cyber Command operatives have begun sending messages to Russian cyber operatives engaged in election interference, informing them that US operatives have identified them and are tracking their activities.[19] Though such deterrence by punishment will remain limited in scope, it could be successfully used in conjunction with societal resilience.

Sweden got an early taste of disrupted food supplies in 1998, when the city of Gävle was hit by a snow storm that left snow averaging 130 centimetres on the ground.[20] Because vehicles were unable to use the streets, the city's supermarkets quickly ran out of food, particularly dairy products. Armed forces tanks and helicopters had transport residents to hospital. An attack on logistics IT systems or sabotage of ports could cause similar chaos, which would be likely to extend far beyond one city. During several recent floods, the UK government has dispatched the British Army to, for example, pile sand bags in order to make roads passable for delivery vehicles.[21] British media reported in July 2017 that the British Army has been told to be on stand-by to deliver food, fuel and medicines to Britons in case of a no-deal Brexit, which may lead to severe delays at British ports.[22] The armed forces are often used as a response to – and deterrent against -- terrorist threats as well. French and Belgian soldiers routinely patrol city streets for that purpose.

The armed forces are a convenient tool in national crises: they possess rare skills and are at the government's disposal. Emergency response at home is, however, not their core task or expertise: combat is. The evolution of threats has exacerbated that capability gap. There is, for example, little the armed forces can do to prevent or stop a disinformation campaign or a hack on a shipping firm. In addition, armed forces are stretched thin. Since the end of the Cold War, most Western European armed forces have been significantly cut, and even the US armed forces have endured personnel cuts. In 1988, the United Kingdom spent 3.6 per cent of GDP on defence; in 2017 the figure was 1.8 per cent.[23] Today the British armed forces are roughly are roughly half the size of their strength in 1980.[24] As DCDC notes, "the reduced military footprint may lead to a delayed military response as units need to travel further to reach an emergency".[25] Indeed, though many Western countries are now increasing defence spending, parliaments are unlikely to increase spending on the armed forces and first responder agencies to the extent that a government could maintain a complete emergency presence across the homeland. Of course, even if a willingness to commit such sums existed, soldiers' and first responders' expertise does not cover central parts of hybrid warfare, such as malign influence campaigns and election interference.

2.1 Existing models of societal resilience and total defence

The answer to the challenge of how to defence the homelands against a blend of conventional and non-conventional aggression lies with a combination of actors: government (including the armed forces), the private sector and the population at large. Put more precisely, the answer lies in cooperation between the government, companies and civil society. During the Cold War, several Western countries – primarily the Scandinavian states – practiced what was known as Total Defence, a set of policies aimed at maintaining continuity of daily life in case of a war in the respective country or its immediate neighbourhood. The

[19] https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html?smtyp=cur&smid=tw-nytimes

[20] https://www.msb.se/Upload/Produkter_tjanster/Publikationer/SPF/Sn%C3%B6kaoset%20runt%20G%C3%A4vle.pdf

[21] https://www.theguardian.com/environment/2016/nov/09/theresa-may-soldiers-army-standby-winter-floods-uk

[22] https://www.thetimes.co.uk/article/army-on-standby-for-no-deal-brexit-emergency-dz3359lrf

[23] https://www.sipri.org/sites/default/files/3_Data%20for%20all%20countries%20from%201988%E2%80%932017%20as%20a%20share%20of%20GDP.pdf

[24] https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7930

[25] Developments, Concepts and Doctrine Centre (2017): UK Operations: the Defence Contribution to Resilience and Security, p 14

concept was initiated by the Swedish government just before World War II, in response to Nazi Germany's Total War strategy.[26]

As the name implies, Total Defence meant that any territorial defence in the homeland involved not just the armed forces but all of society. Specifically, as defined by the Swedish government, Total Defence meant that during times of peace the government created conditions to ensure society would remain operational in case of war or other national crises. In Sweden, Total Defence featured a well-trained and professionally equipped Home Guard that assisted both the armed forces and civilian agencies. In case of a land invasion, Home Guard units would have been a crucial citizen bulwark, whose units – operating in their home regions – would have helped thwart the advance of hostile forces. Companies' critical staff were assigned to emergency roles. Civilian assets, down to relatively simple items such as lorries, were likewise centrally accounted for and assigned Total Defence roles in case of a crisis. Economic defence further entailed, among other things, secure production and storage of strategic goods. The government also maintained work mobilisation plans involving the entire adult population.[27]

Parts of Total Defence remain in existence. Denmark and Norway's volunteer Home Guards, created immediately after World War II, remain well-equipped and well-trained, and successfully fulfil duties ranging from crowd control, evacuation and guarding of crime scenes to assistance of full-time armed forces personnel. Last year's appointment of Major General Eirik Kristoffersen, a fast-rising former Special Forces commander, as commander of Norway's Home Guard (Heimevernet), shows how seriously the Norwegian government takes community-based homeland defence.[28] Though Sweden's Home Guard (Hemvärnet) has, along with the country's professional armed forces, endured nearly two decades of insufficient funding and political attention, the changing security situation has reversed that trend. Sweden is also reinstating and updating other parts of its Cold War Total Defence. In a crisis situation, residents are now expected to be able to support themselves during a national emergency. Last year the Swedish Contingencies Agency (MSB) – the government agency in charge of crisis preparedness, preparation and coordination – received a significant budget increase for 2018-2020.[29] "As a private individual, you also

have a responsibility. Preparing correctly can enable you to cope with a difficult situation, regardless of what has caused it. In the event of a societal emergency, help will be provided first to those who need it most. The majority must be prepared to cope on their own for some time," the MSB told residents of Sweden in the brochure *If War or Crisis Comes*, which was sent to all households in the country in the spring of 2018.

In simple bullet points, the brochure also provides crisis preparedness instructions: which items and food products to always store at home; how to proceed with daily life if the supply of power, water or both; how to identify disinformation; how to receive government announcements during a crisis.

The brochure points out that during a crisis, the following may happen:

- • The heating stops working.
- • It becomes difficult to prepare and store food.
- • The shops may run out of food and other goods.
- • There is no water coming from the taps or the toilet.
- • It is not possible to fill up your car.

[26] http://fokk.eu/files/2017/11/31-Totalfo%CC%88rsvaret-under-Sveriges-kalla-krig.pdf

[27] http://fokk.eu/files/2017/11/31-Totalfo%CC%88rsvaret-under-Sveriges-kalla-krig.pdf

[28] https://forsvaret.no/aktuelt/eirik-kristoffersen-blir-ny-sjef-heimevernet

[29] https://www.msb.se/sv/Om-MSB/Sa-arbetar-MSB/MSBs-budget-2016/

- • Payment cards and cash machines do not work.
- • Mobile networks and the internet do not work.
- • Public transport and other means of transport are at a standstill.
- • It becomes difficult to obtain medicines and medical equipment.[30]

During the Cold War, Sweden's Total Defence would have made a Soviet invasion much more complicated and time-consuming. Sweden's armed forces were, of course, dwarfed by the mighty Soviet armed forces, but the fact that large parts of the civilian population would be engaged in denying the adversary any breakthroughs made invading Sweden less attractive. Sweden's Total Defence would, in other words, have increased the adversary's cost of engaging in aggression.

It is thus clearly both possible and desirable to involve the population in national security. Society can function as a deterrent. It can do so not through deterrence by punishment – the domain of the armed forces – but through deterrence by resilience. That is especially true in a security situation where part of the aggression blend is targeted squarely at civil society.

3 IMPLEMENTATION MEASURES: HOW TO DESIGN DETERRRENCE BY SOCIETAL RESLIENCE

3.1 Concept

Deterrence by resilience does not compete with the armed forces. On the contrary, societal deterrence by resilience complements deterrence by punishment. This is especially true as non-military threats and attacks primarily target the private sector and civil society, not the target country's armed forces, with the goal of weakening the country rather than seizing land.[31] As noted by Roberts and Hardie, "deterrence works best between rational actors who have a mutual understanding in the status quo and who have, to some extent, an intellectual relationship in which they understand each other's motives"[32]. Deterrence by punishment is clearly an efficient model for military action, but with hybrid warfare including non-military elements, defence and deterrence against it should likewise be blended. Indeed, given that non-military elements of hybrid warfare are capable of causing such damage on their own, they clearly warrant a deterrence suited to them: deterrence by societal resilience.

Society is, according to Merriam-Webster's definition 3b, "a community, nation, or broad grouping of people having common traditions, institutions, and collective activities and interests". People rather than institutions are, one could argue, the defining feature of societies. Margaret Thatcher, the former British prime minister, said as much in her famous comment that began with "there's no such thing as society", going on to explain that "there are individual men and women and there are families. And no government can do anything except through people, and people must look after themselves first. It is our duty to look after ourselves and then, also, to look after our neighbours."[33]

[30] https://www.msb.se/Upload/Forebyggande/Krisberedskap/Krisberedskapsveckan/Fakta%20om%20broschyren%20Om%20krisen%20eller%20Kriget%20kommer/If%20crises%20or%20war%20comes.pdf

[31] As Oona Hathaway and Scott Shapiro exhaustively document in The Internationalists: How a Radical Plan to Outlaw War Remade the World (2017), the frequency of land conquests has dramatically dropped since the end of World War II.

[32] Roberts, Peter and Andrew Hardie: Is deterrence a valid philosophical concept for the next twenty years? RUSI Occasional Paper

[33] https://www.theguardian.com/politics/2013/apr/08/margaret-thatcher-quotes

That is particularly true in national security crises, and in the preparation for them. Even though the government can, and must, take on a central coordinating function before and during national emergencies, it cannot look after the well-being of all. This is especially true as many of the targets of potential aggression – for example companies in strategic sectors – are no longer owned by the government but by private shareholders, and many are not classified as critical national infrastructure that qualifies for additional protective measures. Furthermore, as DCDC notes, ageing populations in developed countries "will see increased demand on national infrastructure (housing, transport and utilities) and public services (health, education and social services). As a result, spare capacity may be reduced or lost altogether for national infrastructure and public services to be able to respond or support an emergency."[34] As Mads Ecklon, who leads the Danish Ministry of Defence's total defence efforts, points out in an article distributed to participants in a recent RUSI conference, today the government should act as a facilitator, rather than the sole provider, of societal deterrence.[35]

Deterrence by societal resilience, then, must entail businesses and the population taking an active role as participants in national security. To be sure, businesses already address their security, but they mostly consider attacks and crises a commercial concern, not a national security concern. Furthermore, national security depends on a net of actors acting in conjunction: if they act in isolation it leaves gaps. As Tim Sweijs, Katarina Kertysova and Frank Bekker of the Hague Centre for Strategic Studies note in a recent report on flow security, "although many different state and non-state actors have a stake in flow security, they do not necessarily have or feel the responsibility to provide and maintain that security".[36]

Currently no country possesses a complete societal resilience system. This is a critical gap in our defence posture, and one that is being exploited by our adversaries. The models developed by the Scandinavian countries (as well as, more recently, the Baltic states) do, however, present a highly beneficial starting point for all NATO allies. Philosophically this is a challenging move for governments: it shifts an underpinning belief in deterrence as a passive, dormant posture to an active and dynamic state of mind that reaches across society, where everyone plays a part. With our population and private sector, however, our societies harbour enormous deterrent potential.

3.2 Suggestions for practical measures

An active societal resilience model can take as its point of departure the simple steps included in the MSB's brochure. It might also include Scandinavian-style Home Guards, well-trained and well-equipped to ensure effectiveness and a reputation as a credible citizen force. Ahead of the September 2018, Swedish national elections, the trained civil servants and the wider public how to identify Russian election interference attempts. Deterrence by resilience can and must, however, go much farther.

Consider the March 2017 terrorist attack on Westminster Bridge and the Houses of Parliament in London. Though acting alone, the terrorist managed to create panic among the many ordinary citizens in the area. The stabbed police constable, Keith Palmer, was given CPR by Tobias Ellwood, an MP and junior defence minister, who happened to possess first-aid skills by virtue of having been a British Army officer. Meanwhile, across central London people immediately used their mobile phones to gather information and call friends and family. Similar patterns of behaviour have characterised bystanders' reaction to other terrorist attacks.

While such behaviour is understandable, in a larger attack of the kind a state actor is capable of, such behaviour would be extraordinarily unhelpful. As Ellwood pointed out after the attack, "we must not become

[34] DCDC, p 13

[35] Footnote will be added when the article is published.

[36] https://hcss.nl/news/flow-security-and-dutch-interests

so risk averse and so reliant on our security services that we allow these events to take place".[37] With a critical mass of a country's citizens, or residents, trained in emergency response, an attack on a Western country would be far less devastating.

Adult residents could, for example, be given the option of attending resilience training. A non-weapons curriculum could be designed by the interior ministry or another government department or agency, and could be delivered either by NGOs such as the Red Cross, or by armed forces officers on secondment to the department or agency in charge. The training could involve surviving for 72 hours without food, water, power or mobile communications. It could also involve crisis response: for example, how to act during a crippling cyber attack, which can of course occur in conjunction with a military attack. In such a situation, it would be imperative for the population to generate resilience as the armed forces would have to focus on military response, while first responders would focus on vulnerable members of society.

Furthermore, with malign influence campaigns permeating and weakening our societies, information literacy must be part of citizen resilience training. According to a March 2018 Eurobarometer survey, 85 percent of EU citizens perceive fake news as a problem in their respective countries.[38] While 71 percent are confident that they can identify disinformation, this is a self-evaluation that may be very far from the truth. Given that disinformation campaigns and social media campaigns (the latter usually with the aim of sowing discord between social and/or ethnic groups) can seriously shape a country's public opinion and weaken its resolve in case of a national crisis, information literacy must be part of resilience training.[39]

So must training of government officials involved in elections. A new MSB report documents concerted efforts, some linked to Russia, to influence Sweden's September 2018 national elections in the direction of the far-right Sweden Democrats, a party widely considered a disruptor in Swedish politics. Other efforts were directed at spreading mistrust in the election itself. "There were over 2,000 posts on Twitter that used the term 'valfusk' (election fraud) in the week preceding the election, suggesting that there was a coordinated campaign to seed the idea of a rigged election before the vote had even occurred", the authors report. [40] Alleged Russian interference in the 2016 US presidential election is, in turn, under investigation by Special Counsel Robert Muller.[41]

The objective of resilience training – without the information literacy -- is similar to the San Francisco City Council's SF72 public awareness campaign, which informs residents how to prepare for an earthquake, survive it, and survive the three days following it.[42] However, any member of the public can choose to ignore public awareness campaigns, which is why the MSB's booklet is, by itself, also far from a complete solution. Participation in training is, in fact, vital to the success of resilience training. There are a variety of ways in which the training could be administered. It could be offered as a residential summer camp for all teenagers in a year-group, ideally the summer prior to the last year of secondary education. This would also solve the issue of how to provide productive summer activities for teenagers, and would allow teenagers to interact – while fulfilling important tasks – with teenagers from other part of society. The desire to promote such social cohesion in our increasingly disparate societies has fuelled large parts of the current conscription debate.

[37] https://www.thetimes.co.uk/article/westminster-terror-attack-tobias-ellwood-mp-who-tried-to-save-pc-keith-palmer-tells-of-parliament-security-fears-s5slg9cg7

[38] https://ec.europa.eu/digital-single-market/en/news/final-results-eurobarometer-fake-news-and-online-disinformation

[39] In the UK, Russian internet trolls have, for example, tried to stir up hatred of Muslims (https://www.thetimes.co.uk/article/russian-trolls-top-priority-in-uk-is-stirring-hatred-of-islam-ptlck6nq7).

[40] https://www.isdglobal.org/wp-content/uploads/2018/10/Sweden_Report_October_2018.pdf

[41] https://www.theguardian.com/us-news/2018/sep/14/robert-mueller-trump-russia-investigation-what-we-know

[42] https://www.sf72.org/

Resilience training could also be offered to adults, perhaps through employers. While participation should not be made mandatory, it could be incentivised. Employees could be given paid time off to participate, and employers could reclaim the expense on their taxes. Employees could also participate in training in their spare time, for example through evening courses offered by NGOs. All courses would need to follow a national curriculum decided by the government. Graduates could receive a resilience training certificate that could be valid for five years, and that could entitle them to annual tax credits.

Resilience training for teenagers would solve the question an increasing number of countries including France are attempting to answer by reinstating national service: how to train young members of society to become good citizens. The French initiative, introduced by President Emmanuel Macron, which aims to "enable young people to create new relationships and develop their role in society", will include a one-month placement in a civic institution followed by a voluntary period of three to 12 months in a field related to defence and security.[43] It is, however, unclear what the teenagers would learn in any of the segments. By contrast, resilience training provides a clear purpose in an area that is easily understood by most citizens, and its non-military nature ensures it would be unobjectionable even for those uncomfortable with weapons or the armed forces.

Individual resilience training segments, in particular information literacy, could also be offered separately. Though information literacy may seem marginal to national security, erosion of public trust in societal institutions poses a fundamental challenge to the health of our societies. By convincing segments of the population that governmental institutions, the news media or companies are incompetent or ill-intentioned, especially during a crisis, an adversary can severely weaken the target country's resolve. Such an erosion of trust in institutions that have taken generations to build can also harm the economy, whose performance depends on trust in a well-functioning society. Information literacy training could be offered through evening courses administered by NGOs or media organisations. Again, graduates could receive certificates that would entitle them to tax credits or other benefits.

The benefits of societal resilience extend beyond national security and full-spectrum deterrence. One of Western societies' most troubling current challenges is the discord among its constituent groups, as evident in recent election gains by populist parties. By definition, building societal resilience brings people from different parts of society together.

Building societal resilience, of course, entails expenses to the government. However, considering the strength societal resilience would generate, and the deterrent effect that would follow, the return on investment is enormous.

[43] https://www.bbc.com/news/world-europe-44625625

Authors:

Elisabeth Braw is an Associate Fellow at RUSI and director of the Institutes Modern Deterrence programme. Previously a journalist, she frequently writes commentaries for The Wall Street Journal, The Financial Times, Foreign Policy and other publications. Elisabeth is especially interested in European armed forces and homeland defence issues. She has also been a visiting fellow at the University of Oxford, and frequently speaks at security conferences.

Professor Peter Roberts is director of Military Sciences at the Royal United Services Institute. He researches and publishes on a range of subjects from strategy and philosophy, contemporary war and warfare, military doctrine and thinking, command and control, naval warfare, ISR, professional military education and disruptive warfare techniues. He lectures, speaks and writes on these topics as well as regularly providing advice for both UK and foreign governments.