Building a Wall of Denial Against Gray-Zone Aggression

Elisabeth Braw

APRIL 2021

AMERICAN ENTERPRISE INSTITUTE

Executive Summary

NATO member states and partners today face national security threats that extend far beyond military aggression. Indeed, they are regularly targeted by nonmilitary means, so-called gray-zone aggression. Because gray-zone aggression can include any measures below the level of war, including illegal ones, it is impossible for the targeted countries to deter every act with the threat of punishment.

This means liberal democracies should give more attention to societal resilience. By involving all parts of society in keeping the country safe in case of a crisis, they can signal to adversaries that aggression will not have the desired effect. Today civil society is, in most countries, a largely untapped resource in national security. Countries from Finland to Singapore feature considerable societal participation in national security, but deterrence of gray-zone aggression also offers considerable potential for innovation.

This report, adapted from my upcoming book *The Defender's Dilemma: Deterring Gray-Zone Aggression*, outlines a whole-of-society model for deterrence by denial and proposes measures governments could take or coordinate to incentivize businesses and the wider population to help keep their countries safe. The proposals include community stress testing, voluntary resilience training for teenagers and other demographic groups, and government-industry consultations on national security issues.

Building a Wall of Denial Against Gray-Zone Aggression

Elisabeth Braw

"In case of war, please ring [the bell] twice."[1] In 1939, Rudolf Minger was prepared. The Swiss defense minister's advantage was, of course, that he had a good idea of what sort of attack to expect, and so did his country's population. Defending a country against gray-zone aggression poses a much harder challenge because the targeted country cannot be sure what forms of aggression will be used and indeed who should mount the defense and deterrence.

Deterrence of gray-zone aggression is possible, though it requires a radical shift in liberal democracies' approach to national security, toward a system that involves not just the government but also the private sector and wider society. Collectively, the government and civil society can create a wall of resilience that denies opportunities to aggressors. Together, liberal democracies' governments can also develop deterrence by punishment by playing to their strengths: that they have allies, that their citizens and private sectors can choose to play a part in national security if offered the opportunity, and that their countries have assets foreign governments and leaders desire.

In addition to deterrence, scholars of the field often discuss dissuasion, which denotes deterrence before any action occurs. For the sake of simplicity, this report divides deterrence into two parts: deterrence by denial and deterrence by punishment. This report outlines a whole-of-society model for deterrence by denial.

Civil Society, a Resource

NATO's Article 3, known as its resilience article, reads: "In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack."[2] Even though the North Atlantic Treaty was signed in 1949, NATO never treated resilience as a priority, partly because its member states could rely on the alliance's powerful deterrence by punishment. By contrast, during the Cold War, Sweden and Finland made exemplary use of resilience, creating a wall of denial that signaled to the Soviet Union that an invasion would involve an unpalatable cost-benefit calculus.[3]

NATO did increase its focus on Article 3 at its 2016 Warsaw Summit, when it adopted the so-called seven baseline requirements for civil preparedness.

1. Assured continuity of government and critical government services;
2. Resilient energy supplies;
3. Ability to deal effectively with uncontrolled movement of people;
4. Resilient food and water resources;
5. Ability to deal with mass casualties;
6. Resilient civil communications systems;
7. Resilient civil transportation systems.[4]

As NATO officials Wolf-Diether Roepke and Hasit Thankey note, "Resilient societies . . . have a greater propensity to bounce back after crises: they tend to recover more rapidly and are able to return to pre-crisis functional levels with greater ease than less resilient societies."[5]

With whole-of-society gray-zone threats targeting them, liberal democracies must similarly create a whole-of-society wall of denial as the bottom of their deterrence pyramid and form part of countries' general deterrence. (As discussed in my previous AEI reports, deterrence by punishment is more useful in targeted and tailored deterrence, in which a country shapes its messaging to other countries, groups, and prospective acts of aggression.)[6]

A whole-of-society wall of denial is a radically different approach from the one most governments currently maintain. Except for papers about Sweden's and Finland's Cold War total defense, the concept has also not been comprehensively explored in academic papers. In their excellent gray-zone report, Lyle Morris et al. propose "a whole-of-government approach" with a range of government initiatives to dissuade rivals from engaging in gray-zone aggression. The proposed initiatives include

> continu[ing] to reaffirm, through regular senior leader statements and official policy documents, the U.S. commitment to formal allies in Europe and Asia and back[ing] these statements with enhanced participation in bilateral and multilateral forums to deal specifically with such gray zone tactics as cyberattacks and disinformation. . . .
>
> The United States could undertake a major diplomatic initiative, coordinated through the State Department and U.S. embassies, to reinforce the international legal implications of gray zone aggression.[7]

Multilateral contacts certainly ought to be strengthened. As Niklas Karlsson—a Social Democratic member of the Swedish parliament—pointed out, Western governments should "make sure that foreign policy is the first line of defense." He also noted that "the UN and the Council of Europe have been languishing for some time. In the '90s, institutions like these were essentially demoted to a secondary role. Now they need an upgrade again."[8] Further, leaders of Western countries and their adversaries must maintain a constant dialogue. This will help the countries not only build cooperation wherever possible but also reduce the risk of misunderstandings and resulting security dilemmas.

The UK government's Fusion Doctrine from 2018, too, foresees an effort exclusively undertaken by the government.

> This approach will ensure that in defending our national security we make better use of all of our capabilities: from economic levers, through cutting-edge military resources to our wider diplomatic and cultural influence on the world's stage. Every part of our government and every one of our agencies has its part to play.[9]

In its *National Security Capability Review* from 2018, the UK government also addressed gray-zone aggression, explaining that

> many adversaries seek to do us harm or subvert us in less destructive ways, calculated to avoid provoking an armed response. We will seek to raise the cost of their malign behaviour, restrict and reduce it using the full range of capabilities available to us. Some of the many capabilities enhanced as a result of SDSR [the Strategic Defence and Security Review] 2015 include the new powers in the Criminal Finances Act 2017 to recover criminal assets and our offensive cyber capabilities to detect, trace and retaliate in kind.[10]

The UK government labeled this innovative approach "modern deterrence."

Again, no role was foreseen for civil society. Indeed, most Western countries appear not to consider the potential available in civil society even though most of them had some form of civil defense during World War II and in the early Cold War years. In World War II Britain, for example, citizens participated in the war effort in a plethora of roles, such as bike messenger, fire watcher, rest center operator, first aid helper, search-and-rescue member, and air raid warden. This system continued after World War II, somewhat modified and under the name Civil Defence Corps. Although the corps was led by the government and designed for wartime use, its members naturally used their skills during everyday contingencies. The Civil Defence Corps was disbanded in 1968.[11]

Civil society could play an even more pivotal role in defense against today's and tomorrow's gray-zone aggression precisely because the aggression is primarily directed against civil society. When trying to improve defense and deterrence while leaving society out, governments practically guarantee they will be overstretched while leaving civil society—individuals, businesses, and other organizations—passive observers of their own fate. Even if a government of a liberal democracy wanted to extend itself to form an omnipresent wall of denial while signaling punishment to would-be aggressors, the costs would be prohibitive, and the effort would at any rate be ineffective. This is one reason no government has tried to extend a cyber-protection umbrella over the entirety of its society.

Indeed, because defense should also aim to deter, a whole-of-government approach would signal that a vital part of society does not wish to be involved or is considered a liability by its own government. This not only indicates weakness but also practically invites adversaries to target civil society. If the private sector is not involved in government-coordinated resilience, its absence signals to a country's adversaries that they can target businesses. The same is true for the citizenry.

Hostile states monitor involvement in resilience efforts—and lack thereof. Precisely because the West's adversaries are adept at spotting and exploiting weaknesses, the ones with both capability and intent will use the opportunities offered to them. The existing results illustrate the damage: cutting-edge businesses lost, others coerced, academic integrity in doubt, and citizens who have lost faith in their countries' institutions.

Governments may not even be best placed to defend countries against all forms of gray-zone aggression. While governments—with their monopoly on violence—should defend their countries against attacks involving sustained use of force, it is unclear how they alone could convincingly defend their countries against subversive investments, coercion of businesses, or interference through academia and popular culture. Ole Weaver defines societal security as "the ability of a society to persist in its essential character under changing conditions and perceived or actual threats."[12] This is clearly the baseline liberal democracies' governments and civil societies must jointly be able to muster. Governments, meanwhile, must clearly lead in deterring illicit forms of gray-zone aggression such as border alterations and intellectual property (IP) theft.

In a major shift from its previous policy, in its 2021 *Integrated Review*, the UK government embraced the whole-of-society concept. In his foreword to the review, Prime Minister Boris Johnson writes that "COVID-19 has reminded us that security threats and tests of national resilience can take many forms,"[13] and the review lists as a priority action

> to establish a "whole-of-society" approach to resilience, so that individuals, businesses and organisations all play a part in building resilience across the UK. We will seek to develop an integrated approach, bringing together all levels of government, CNI [critical national infrastructure] operators, the wider private sector, civil society and the public.[14]

A highly innovative step as part of this whole-of-society approach is the UK government's intention to create a civilian reserve.[15]

This is precisely the right approach to take. By involving all parts of society, targeted countries can minimize the opportunity for gray-zone aggression. The collective resilience can signal to adversaries that their cost-benefit calculus will be negative: a continuation of Sweden's and Finland's Cold War deterrence by denial, which signaled to the Soviet Union that while the two countries might be easy to attack, they would significantly reduce the winner's spoils and make sure aggression involved more effort than the Soviet Union wanted to expend. The same collective resilience will, of course, also reduce the effect of gray-zone aggression should the deterrence signaling fail.

The point of departure must be to treat the citizenry as a resource rather than a fragile entity whose only attribute is the need for protection. As Carl Rådestad and Oscar Larsson observe, "Activated citizens are not necessarily silent recipients of services, but may also become activists and create pockets

of resistance and shift the burden of responsibility away from themselves during and after emergency situations."[16]

By empowering the population, governments can achieve two goals. The public—both the private sector and the citizenry—assumes some of the duties the government would otherwise have to execute, which frees up the government to focus on duties it alone can perform. In addition, civil society becomes an integral part of national security, thereby reducing gaps adversaries would otherwise seek to exploit. This approach also creates reserves of experts, increases governments' freedom of action, and provides resource strategies the government may wish to pursue. This way, governments and their societies form a combined shield to deny adversaries the benefits they seek and negatively influence the adversaries' cost-benefit calculus.

Such an approach clearly involves a major shift in both policy and practice. While most armed conflicts are whole-of-society efforts, whether the public has chosen to participate, in peacetime, liberal democracies' civil societies are rarely asked to participate in national security. Except for a small number of countries such as Finland, governments have tried to form a shield over their civil societies instead of building a combined shield integrating their civil societies. Western governments' challenge today is to engage citizens and organizations that have previously had minimal interaction with national security, thus creating a credible bottom layer of the deterrence pyramid.

Before the UK government's significant shift with its 2021 Integrated Review, some other larger countries had floated rather more modest ideas. For example, Germany's 2016 national security white paper called for

> whole-of-society resilience and thus comprehensive defence capabilities. . . . This includes better protection of critical infrastructure, reduced vulnerabilities in the energy sector, civil defence and disaster control issues. . . . Politicians, the media and society must all help when it comes to exposing propaganda and countering it with facts.[17]

Yet such calls were mostly not followed by deeds. In fact, while the World War II generation is habitually been lauded as "the greatest generation," since the end of the Cold War, most Western governments have been wary of asking their citizens for even the most rudimentary contribution to national security.

This reluctance was certainly influenced by the early 21st century's prevailing neoliberal mood, in which citizens increasingly saw—and were encouraged to see—national security as a service provided by the government in exchange for their taxes, not a collective undertaking. In addition, the 21st century's largely peaceful decades in the homeland did not require much societal involvement in national security. Yet governments may also have lacked confidence in the citizenry's abilities. Larsson and Rådestad note that

> social constructions regarding how individuals behave in a crisis are now often based upon the assumption that people panic and desperately need the support of public authorities. . . . One common assumption is that crisis situations are typically accompanied by outbreaks of lawlessness and social chaos due to the irrational behavior of helpless individuals, who almost immediately return to a Hobbesian state of nature.[18]

The combination of citizens largely left to pursue their individual happiness and being enticed to conduct an increasing number of tasks (from airport self-check-ins to supermarket self-checkouts) while not being entrusted to participate in or even understand matters of their country's security is paradoxical and baffling. Indeed, it stands to reason that governments can incentivize personal responsibility in matters of national security just as companies do in their respective areas. Indeed, it is highly likely that if given the opportunity to be part of national security in the widest sense—that is, helping keep their families, communities, and the country safe—the majority of citizens would prefer feeling empowered rather than helpless during crises big and small.

During the Cold War, virtually all European countries had mandatory national service for men, but

this was mostly phased out after the Cold War ended. Sweden also dismantled its impressive total defense system and thus jettisoned not just the involvement of citizen volunteers but also the private sector. Since then, Sweden has introduced highly selective military service for men and women, Norway has expanded its highly selective military service to women, and Lithuania has introduced a less selective model.[19] Although these models have considerable benefits, as do related models in other countries such as Denmark and mandatory military service in Finland and Estonia, they clearly do not constitute comprehensive citizen participation in gray-zone defense and deterrence.

Because it did not dismantle its Cold War total defense, Finland remains the Western country best set up for gray-zone defense. Yet not even its combination of reserves comprising all former conscripts and therefore a cross-section of society, newer initiatives such as disinformation literacy training in schools,[20] a national defense course, and government first right to buy of properties in sensitive locations provide sufficient deterrence of gray-zone aggression in its various incarnations.

Creating Societal Resilience to Form Deterrence by Denial

Perhaps unsurprisingly, the Nordic countries remain ahead of the curve in making civil society part of national resilience and thus deterrence by denial. In its 2018 Security Strategy for Society, the Finnish government explains that the country's "preparedness is based on the principle of comprehensive security in which the vital functions of society are jointly safeguarded by the authorities, *business operators, organisations and citizens*."[21] (Emphasis added.) Finland also recognizes the growing importance of the private sector even compared to the Cold War, a result of privatization of critical national infrastructure: "Business operators are playing an increasingly important role in the preparedness process. In particular, companies will continue to play a key role in the process of ensuring the functioning of the economy and the infrastructure."[22] Sweden is (partially) rebuilding its total defense: The all-hazards contingencies agency MSB is a global leader in public education and crisis coordination, and in March 2021, the government announced it will create a new agency for psychological defense.[23] It has also updated its Cold War total defense exercises that involved the armed forces, all levels of government, auxiliary defense organizations, and businesses linked to the national defense effort. The last such exercise took place in 1987, but in 2019, Sweden resurrected the concept with a new exercise, Total Defense Exercise 2020.[24] The focus of the total defense exercises, however, remains conventional aggression.

Denmark, in turn, explains in its *Foreign and Security Policy Strategy, 2017–2018*, that the government intends to "reach out and strengthen Denmark in collaboration with civil society organisations, the business community, universities and think tanks. Denmark is at its strongest when we stand together."[25]

The Nordics are joined by their Baltic neighbors. In its *National Security Concept 2017*, the Estonian government states it aims to "increase peoples' [sic] perception of security and enhance their ability to evaluate various threats and factors that influence security, as well as their ability and readiness to counter such threats."[26] While not as all-encompassing as Sweden's Cold War total defense, Estonia's whole-of-society model includes, among other things, a cyber defense unit, in which civilian IT experts volunteer their time defending the country against cyber threats.[27] Latvia's comprehensive national defense, initiated in 2018, similarly highlights the role of civil society. In 2020, for example, the country published a leaflet called *72 Hours*, similar to Sweden's *If War Comes*, which Sweden itself updated and reissued as *If Crisis or War Comes* in 2018.[28]

Soon after the leaflet's launch, the country's defense minister, Artis Pabriks, wrote:

> Covering a broad range of crises, "72 hours" therefore prepares society for catastrophes we cannot specifically predict, like the coronavirus pandemic that the world is facing right now, and includes instructions on actions to take, details on the civil defence warning system and information channels, as well as

> information on water and food reserves and primary health care. It has to be emphasised though, that preparedness cannot avert crises; what it can do is reduce the extent of possible negative consequences.[29]

"Catastrophes we cannot specifically predict" and "reduce the extent of possible negative consequences"[30] are precisely what every country targeted by gray-zone aggression should strive for by using every lever at its disposal. Indeed, because gray-zone aggression—unlike traditional military aggression—targets countries regardless of their geography, it is a wake-up call for countries located far from potential military aggressors. Such countries, including the United States, have in recent decades had the luxury of treating national security as a concern that can be addressed almost exclusively by the armed forces and other parts of the government. It points to a changing mindset that the US Cyberspace Solarium Commission proposed that Congress "codify the concept of 'systemically important critical infrastructure,'" which would guarantee operators US government support—and create and fund a joint collaborative environment for the sharing and fusing of threat information.[31]

In other countries that have traditionally been less inclined toward whole-of-society efforts, the direction is also changing somewhat. In 2019, France launched a new form of national service, initially on a pilot basis. During the monthlong program, 16-year-olds are taught skills such as map reading and spend time doing community service. "What's missing is a moment of cohesion . . . of youth coming together from different parts of France, from different social backgrounds, sharing their experiences and their commitments for society and the country," Junior Education Minister Gabriel Attal explained when the initiative was launched.[32] While the training thus primarily has a social objective, it could help contribute to resilience. So could Germany's small Your Year for Germany program, launched in 2020, in which young Germans can spend six months training with the armed forces and six months assisting in homeland protection in their home regions.[33]

Such initiatives alone, however, do not create deterrence, and this is not the intention. A more focused effort is Latvia's Comprehensive Defense Approach. As part of this strategy, in 2019 the Latvian government invited more than 90 key companies and nongovernmental organizations (NGOs) to its annual whole-of-government crisis management exercise. The policy also features a national security curriculum for 16- and 17-year-olds. As part of the curriculum, introduced in 2019 and gradually rolled out since then, teenagers spend one hour each month learning practical skills such as map reading and basic military skills and the foundations of Latvian national security and the threats facing it, and they can participate in voluntary summer camps.[34]

Involving Citizens

How, then, do we populate the bottom layer of the deterrence pyramid to help form a wall of denial that can change a gray-zone aggressor's cost-benefit calculus? Like the bottom layer in the food pyramid with its bread and potatoes, the bottom layer in the deterrence pyramid are the functions that may seem trivial but are nonetheless central to the organism's functioning.

Unlike military aggression, which most citizens of liberal democracies have not experienced and are unlikely ever to experience, gray-zone aggression is very real. Americans and others are now aware that disinformation harms their democracies. Citizens everywhere have seen a pandemic dramatically disrupt their lives and realized that such disruption can happen again, caused again by Mother Nature—or by a hostile state. They know that an internet or electricity outage will immediately affect their daily lives. At the very least, since spring 2020, when COVID-19 created shortages of personal protective equipment and stockpiling led to empty shelves in supermarkets, they are familiar with the fragility of supply chains. Indeed, liberal democracies' openness combined with the convenience trap—Western societies' enormous and growing dependence on digitally powered conveniences, which increases their vulnerability—means ordinary citizens today are exposed to national

security threats in a way they have not been during previous nonwar periods.

Precisely because gray-zone aggression affects ordinary citizens, it is in their interest to limit its effect. This is true also for citizens who may have no interest in national security or who may be uneasy about military activities. But for citizens to want to do their part, governments must be transparent about the threats and aggression facing the country. This involves sharing and articulating information in a way that most governments are unaccustomed to. If they do not, many citizens are likely to suspect that the asked-for involvement is driven by special interests, not genuine needs. If a majority of Swedish citizens during the Cold War had mistrusted government information about threats facing the country, hundreds of thousands of them would not have joined auxiliary defense organizations, and it is unlikely that one of them would have spotted and reported the Soviet U-137 submarine that, in 1981, ran aground off the coast of Sweden.[35]

Public-Awareness Campaigns. Governments can build on this close link between citizens and new national security threats by offering training to different groups of citizens. The first step by any country targeted by gray-zone aggression must certainly be to educate its public about it in the same vein as Sweden's Cold War *If War Comes* and today's *If Crisis or War Comes*, Latvia's *72 Hours*, and earthquake zones' public-awareness campaigns. While citizens may have heard of disinformation disasters such as the January 6 assault on the US Capitol or may have seen supermarket shelves empty during the first weeks of COVID-19, this does not mean they understand national security threats, their potential role in minimizing the effect of these threats, or how to stave them off altogether.

Sweden and Finland made virtually every resident a participant in their Cold War efforts to deny the adversary advantages. This began at the most rudimentary level: knowing how to identify a national security contingency, prepare for it, and respond. *If War Comes* was that most basic part of resilience. Current governments can use this model, adapting the information to match what they consider their most critical national security threats. Such information is necessary even though many citizens of advanced societies consider themselves well educated. While they may indeed be well educated, it does not mean they understand contemporary risks to their societies. Regarding information and disinformation, Ojars Kalnins, a Latvian member of parliament, observed:

> People need to be educated about what our adversaries' efforts are. This also creates a dilemma: how do you maintain free speech when people spread lies online? I recently got into a bit of an argument with an American friend of mine, who complained that things he writes on Facebook are being taken down. There's no right to have everything you say published! Many years ago, I used to write letters to the editor. Sometimes they'd get published, sometimes not. You didn't have the right then to get anything you wanted published and you shouldn't have any such right now either! I'm also concerned about young people's tech skills. They're very savvy about the technology but not about the content.[36]

In Lithuania, the country's public-service broadcaster, Lithuanian Radio and Television (LRT), now educates the public through national security–related programming. Monika Garbačiauskaitė-Budrienė, LRT's CEO, explained that

> together with the Journalism Development Network [a global network of investigative journalists], LRT has launched the fact-checking project *Facts* on its web portal, which address cases of news manipulation and educates people in how to recognize cases of misleading or manipulative information.[37]

She also highlighted the show *Battlefield*, which is "dedicated to security and defense topics and among them regularly covers issues of information security examining cases of information influence and manipulation."[38]

News organizations could, in fact, play a crucial role in educating the public beyond their current role in providing news while helping increase trust in vetted news and societal institutions. Just as

elected politicians regularly meet with constituents in their constituency offices, thereby maintaining and strengthening a vital link, news organizations could launch similar open houses in cities where they are based or have offices, on a pop-up basis, in other cities and towns. Such encounters with journalists, in which the guests could also participate in news meetings where the next bulletin or newspaper edition are planned, would allow ordinary citizens to learn how news is made and could help dispel concerns that journalists collectively provide slanted or inaccurate coverage.

Indeed, because distance and lack of exposure breed fear, such encounters would help many ordinary citizens (and by extension their friends and social media contacts) realize that news media are not inherently nefarious. Increased trust in professional news organizations would, of course, reduce the opportunities for disinformation to spread.[39] Conversely, the interaction would help journalists better understand ordinary citizens' concerns.

Considering that lack of access to quality journalism also increases the gray-zone attack surface provided by social media, governments—working with news organizations—could also launch voucher schemes that would give residents free access to a news outlet of their choice for a certain period.

While learning about national security threats is never enjoyable, doing so while having a chance to prepare is certainly preferable to learning about them when they have already struck. Indeed, judging from real estate prices in earthquake zones with frequent public-awareness campaigns such as Tokyo[40] and San Francisco,[41] keeping citizens informed about risks does not cause panic.

Societal Stress Testing. Governments could also introduce societal stress testing. After the 2008 financial crisis, governments introduced stricter stress tests for banks.[42] Thanks to this comprehensive stress-testing regime, governments, borrowers, and the wider public can be certain that the global financial system will survive any future financial crises relatively intact. This creates confidence in the banking system.

The same model could be used for the population to test and improve resilience for, say, outage of internet, water, or electricity, or the spread of dangerous viruses. If local authorities, working with the relevant providers and retailers, shut off water, electricity, certain food items, or the internet on apparently random dates throughout the year, residents would learn to prepare for such situations and would know what to do while it was happening. Regular stress testing would help citizens gain enough preparedness skills that they would not panic in case of a real crisis. Indeed, citizens could regularly stress test themselves for various disruptions to daily life. Authorities could highlight such crisis proficiency, to both reassure the country (as is done with bank stress testing) and change a prospective attacker's cost-benefit calculus.

In 2019, Fort Bragg US Army base in Georgia conducted precisely such a stress test; the commander turned off the power and instructed the base's 50,000-some soldiers and officers to continue their daily work without providing further details.[43] While stress testing for gray-zone aggression is a new concept, earthquake zones have long practiced earthquake drills.[44] Texas residents, meanwhile, would certainly have had a less disastrous encounter with power outages during the 2021 winter storm[45] had local authorities conducted stress testing for such a contingency.

Resilience Training Courses. More comprehensive training could be provided through government-supported resilience training courses. One model would be to offer such courses to teenagers during school breaks, either in one chunk of three to four weeks during the summer break or as one-week segments during other school holidays. The training—offered in a residential setting on, for example, university campuses during university breaks—would be voluntary and feature basic resilience skills including information literacy, crisis preparedness, and response during crises ranging from pandemics to supply chain disruptions.

While the government would fund the courses and set the curriculum, the training could be delivered by NGOs such as the Red Cross, high school

teachers with specialized skills, and military officers on secondment and thus teaching in a civilian capacity. Upon completion of the course, participants could receive—depending on the respective country's system—university application points or other credit for university applications or tax credits for those planning to enter the labor market immediately after completing secondary education. The course certificate awarded upon completion of the course could be kept current through refresher courses. Participants keeping their certificates current could also receive tax credits. Because the curriculum would reflect current gray-zone threats, the curriculum of the initial course and refresher courses could be continuously updated to reflect evolving gray-zone forms of aggression.

In addition to offering a meaningful activity to late teens during their school breaks, the courses would be an opportunity for teenagers from different backgrounds to interact based on a crucial and highly relevant subject. While teenagers from different backgrounds also meet in school, schools remain an insufficient tool of societal integration. Resilience courses—much like past generations' national service—would increase the opportunities for interaction across societal groups and thus for societal cohesion. This is especially important because liberal democracies' adversaries are apt at identifying and exploiting gaps in societal cohesion. During the 2016 US election campaign, Russia's social media interference campaign especially targeted black voters.[46]

Graduates of the training would be entered into a central database and would be available to assist emergency services and crisis agencies, assisting rather than displacing firefighters, ambulance crews, Red Cross workers, and other responders. By virtue of being registered in the database along with their addresses, they would be able to attend follow-up training in their local area and thus keep their status as resilience aiders current. In addition, just as government authorities have introduced apps for COVID-19 tracing, they could launch "citizen aider" apps in which trained citizens would receive requests for responders in their local area and could indicate their availability to assist.

Resilience training would not have to be limited to teenagers. While 17- and 18-year-olds are physically stronger than most other citizens are and an easier group to bring together, citizens' impromptu willingness to help during COVID-19 and various other crises from hurricanes to forest fires demonstrates enormous potential for communal efforts—but such efforts have to be organized *before* a crisis. Indeed, resilience training could be a way to harness and build on the skills not just of 17- and 18-year-olds but of other groups as well, including retirees, people on nontraditional career paths who may be working part-time or freelance, people who have gaps between full-time jobs, or even people in full-time employment. The former groups often feel marginalized, having (perhaps temporarily) left the labor market. Resilience training would benefit not just them and the social fabric of society but also contingency management and therefore deterrence by denial. The rapid spread of the Q-Anon conspiracy theory[47] is fueled by many citizens feeling left out of a society that seems to be mysteriously run by an inner circle, with ordinary citizens left to be observers of their own lives. Opportunities to play a constructive role in the community, alongside fellow citizens, could also counteract that.

In addition, every societal group would benefit—in skills acquired and social connections established—from participating in resilience training, and society would benefit as a result. In the case of people in full-time employment, training would best be delivered during weekends, much as is the case with armed forces reserves. All groups should be invited to attend refresher courses to keep their resilience status (and thus tax credit and eligibility for crisis responder duty) active.

This would also aid crisis response, as services needing assistance could quickly reach local graduates of the training; that is, there would be an advantage not just of speed but also of expertise in the local area. This can be contrasted with existing crisis response efforts, in which the armed forces frequently have to send active-duty personnel, reserves, or (in the US) the National Guard to assist local agencies. The Home Guards in Denmark, Norway, and Sweden

are currently the closest organized citizen-responder model, but because Home Guards involve military elements, they may not be palatable to all citizens. The Home Guards are also more highly trained than the citizen responders proposed here would be.

Citizens already help during crises. When COVID-19 struck Britain, the government issued a call for 250,000 volunteers to join a newly created "NHS army" to help vulnerable citizens. In response, 750,000 Britons immediately signed up,[48] but because the call was issued during a crisis, the government lacked capacity to accommodate most of them. That the UK government also failed to register the volunteers' details for future contingency needs demonstrates the gap between citizen willingness to assist and organized opportunities available.

Indeed, the challenge in involving civil society in crisis response is that, apart from the people with previous work experience in the respective field, volunteers mostly lack the skills for the tasks. That leads to situations in which well-intentioned offers pose a burden for emergency workers instead of helping them. Resilience training would address the recurring gap between citizen willingness to help and skills to do so while signaling to adversaries that the public's involvement would reduce the effect of any attack.

Germany's Technisches Hilfswerk, a government contingencies agency that includes a volunteer force of some 80,000, assists in contingencies ranging from bridge ruptures to water contamination,[49] and many other countries have some form of disaster-relief volunteer organizations. In New Zealand, for example, students assisting victims of the 2011 earthquake subsequently founded the Student Volunteer Army, whose members assist fellow citizens during a range of crises.[50] In Sweden, meanwhile, large numbers of people have in recent years joined volunteer search-and-rescue organizations such as Missing People, whose members are trained for the task and assist the police. These groups, however, have specific missions and membership and do not claim to by themselves form comprehensive societal resilience.

Singapore, a whole-of-society pioneer, takes a somewhat different approach, with total defense taught to the public on each Total Defense Day (which is on February 15, marking Singapore's fall to the Japanese in 1942). On each Total Defense Day, the "Important Message" signal of the public warning system is sounded to commemorate the day and remind the public of the system's different meanings. As the Singapore Civil Defence Force explains, Total Defense Day "is also an occasion to refamiliarise our people with the modern defence strategy of 'Total Defence' which Singapore has adopted to ensure our continued survival and security."[51]

While communal activities are available to residents of all liberal democracies, civic participation is declining. In *Bowling Alone*, Robert Putnam documents this trend in the United States.[52] In addition, the rate of single-person households is increasing. For example, in Britain between 1999 and 2019, the number of people living alone grew by a fifth from 6.8 million to 8.2 million.[53] This fragmentation, atomization even, of society creates even more opportunities for gray-zone aggression. If a person, family, group, or business does not feel connected to wider society, they are unlikely to act in the interest of society. Through resilience training, citizens could learn practical skills that benefit themselves and their families and feel part of a national effort to keep their countries safe from threats that could cause real harm to their own lives.

Paradoxically, societal involvement in gray-zone defense and deterrence is thus a burden that creates purpose. In a society in which fewer people spend their working lives in uninterrupted career progressions than was the case two or three decades ago and in which artificial intelligence has replaced many tasks humans previously conducted, individuals need ways to express their contribution and therefore their place and value in society. Countries need societal resilience as part of deterrence, but the societal resilience effort also brings the enormous benefit of aiding societal cohesion.

The most important benefit of the resilience training, however, is that countries would have at their disposal a critical mass of people who would be not just alert citizens but also able active participants in emergencies ranging from serious national contingencies

to minor ones such as traffic accidents. Because the training would be nonmilitary and involve no weapons, it would also be palatable to citizens who may be uneasy about the armed forces but who do want to make a difference in their own lives and that of others. This citizen resolve, too, would help change adversaries' cost-benefit calculus.

Selective National Service in All Parts of Government Involved in Crisis Management. Another step on the ladder of involvement in national security is selective national service for secondary school graduates in all parts of government involved in crisis management. This concept, first proposed in an October 2019 report,[54] builds on the selective national service model Denmark, Norway, and Sweden use.[55] After the Cold War, Norway gradually reduced the number of young men doing military service. By 2016, about one-third of the country's around 30,000 male 19-year-olds were accepted for military service. That year, the country switched to gender-neutral national service, meaning all members of a year group are now assessed for national service even though the armed forces' needs remain the same, about 8,000 per year. In 2019, 7,996 young Norwegians were selected for national service[56] in different parts of the Norwegian armed forces, out of 59,234 19-year-olds.[57]

This selectivity, which equals a 13 percent acceptance rate, makes Norway's national service highly attractive to young Norwegians, and having served is an exceptionally strong entry on their resumes. Selectivity—a necessary path to pursue because the end of the Cold War meant Norway, like other countries, no longer needed large conscription-based armed forces—has thus turned national service from a burden on every Norwegian man into a highly desirable activity for which the Norwegian armed forces can select top-achieving young men and women. The success has made national service a prime source of recruitment for the armed forces: Around 25 percent of national service participants now opt for a military career.[58] In addition, the armed forces' attractiveness is reflected in surveys of favorite prospective employers among university students. In the 2020 survey, the armed forces ranked fourth among IT students, eighth among engineering students, 12th among liberal arts students, and 15th among business students (ahead of enterprises such as KPMG, the Oslo Stock Exchange, and Norway's Ministry of Finance).[59]

Other countries could build on this model, in which a national security need that at any rate does not require great quantities of people becomes, by virtue of its selectivity, an attractive proposition for young people. To meet the needs of gray-zone defense and deterrence, such a model should not be limited to the armed forces. Instead, all parts of the government involved in some aspect of national security—ranging from the armed forces to provision of health care—should be able to select a small group of secondary school graduates for training in a range of specializations. Sweden and Denmark have already expanded their national service systems to feature cyber specialization.[60]

The model could be set up similarly to the Norwegian one.

1. In their final year of secondary education, all young men and women are invited to the first round of selection, in which they fill out online self-assessments.

2. Based on the self-assessment results, a smaller number is invited for in-person tests covering their intelligence and physical and mental capabilities and interviews with the government agencies involved.

3. Based on these tests, the government agencies involved—which can range from specialized military units to agencies providing health care—select the candidates of their choice.

4. Those selected are invited to spend 12 months in fast-track training and service with the respective government agency.

5. Upon finishing their service, they are entered into a reserve corps for the respective agency, which the agency can activate during crises.

Such a system would mean that all relevant parts of the government could access a reserve of specialists and would not need to improvise during crises. While the arrangement mirrors the armed forces' reserves model, the national security reserves' main attribute would be their specialization, not large numbers.

Conversely, it would be an opportunity for every member of an annual cohort to be assessed on their individual merit, not their educational background. As a result, it would offer opportunities for young people who may—perhaps because of their background or lack of access to a top education—otherwise have been overlooked by employers. The training provided during the first year and refresher training would provide them with valuable skills and, by virtue of having been selected for the program, would help them stand out on the labor market. While its prime purpose should obviously be defense and deterrence, selective national service would clearly also aid social mobility.

Informed and engaged citizens can make individual choices in the gray zone. They can decide whether to support a celebrity-endorsed firm with links to a hostile regime. They can choose to attend resilience training that will help them, their local communities, and the country in a crisis. They can seize the opportunity if offered a place in a highly selective national service program. Such involvement backs up whole-of-government efforts and helps build—and signal to adversaries—a wall of denial. In their efforts to deter gray-zone aggression, liberal democracies will benefit from empowered citizens. Indeed, the urgent issue of deterring gray-zone aggression through citizen participation may help liberal democracies counter the dangerous fragmentation first documented by Putnam.

The citizen engagement also offers a side benefit in foreign policy: with a corps of citizens trained in basic resilience and specialized tasks, and with both groups part of a crisis response, Western governments could deploy volunteers from both groups to nonmilitary contingencies in other parts of the world. This would benefit the affected countries and help increase Western soft power, particularly as the West's rivals make no such efforts.[61]

Involving the Private Sector

During his Senate confirmation hearings to be US secretary of defense, General Motors' (GM) president, Charles E. Wilson, was asked whether he could make a decision that was in the interest of the United States but could harm GM (in which Wilson would retain stock). He responded:

> Yes, sir; I could. I cannot conceive of one because for years I thought what was good for our country was good for General Motors, and vice versa. The difference did not exist. Our company is too big. It goes with the welfare of the country. Our contribution to the Nation is quite considerable.[62]

What is good for GM is good for the United States: Similar sayings exist in many other countries. What is good for Volvo is good for Sweden. What is good for Nokia is good for Finland. What is good for BMW is good for Germany. During the Cold War and in previous eras, business leaders like Wilson also felt an obligation to their respective home country's well-being, if nothing else because their businesses' success depended on their country's success. In addition, with rare exceptions, executives were citizens of the countries in which their companies were based.

This generated some degree of allegiance to their respective home governments, even when businesses were under no legal obligation to show allegiance. In a 2007 interview, Helmut Schmidt—a Social Democrat and chancellor of Germany from 1974 to 1982—recounted one such example. In the late '70s, he told the interviewer, the Iranian government had wanted to buy a sizable stake in Daimler-Benz.

> The ayatollah was waiting in Paris, and it was obvious that there would be a change of power. . . . I found it inappropriate that the pearl of German industry, which is what Daimler-Benz was, would end up in Iranian hands. I thought, this has to be prevented.[63]

Schmidt proceeded to ask Deutsche Bank, then a distinctly German company, to buy the stake.

> I said, it is in the patriotic interest that you buy this stake. You may have to keep the stake for many years . . . but you have to do it. And because they were good patriots, they did.[64]

Globalization has ushered in a new reality. Globe-spanning conglomerates may have their headquarters in a Western country but be led by top executives of different nationalities. McDonald's, perhaps the world's most-recognized symbol of the United States, has a C-suite that, among others, features Britons and a Pole.[65] Top executives of the 21st century have included Indian-born Indra Nooyi at PepsiCo; Irishman Neville Isdell at Coca-Cola; German Klaus Kleinfeld at Alcoa, the US aluminum giant; British-Indian Anshu Jain, Briton John Cryan, and Swiss-born Josef Ackermann at Deutsche Bank; Indian-born Singaporean citizen Rajeev Suri at Nokia[66]; and the Swede Ola Källenius at the helm of Daimler.[67] In addition, companies ranging from global behemoths to midsize firms have operations in various countries and supply chains spanning even more countries. It would be a valid question to ask whether new market leaders such as Facebook, Netflix, and Spotify in any way represent their home countries or simply happen to be based there. Indeed, one could argue that some firms today are more powerful than many nation-states are.

Precisely such firms and indeed a cross-section of Western private sectors are, as detailed in previous chapters, finding themselves unwitting participants in the increasing geopolitical confrontation. This presents a new reality for a generation of business leaders who have primarily viewed countries as markets or sources of production or supplies, not as sources of mutual confrontation. The dilemma facing businesses is: Can the "Davos Man" approach be reconciled with the new reality of operating in a world of gray-zone aggression?

It can, if globalized businesses help liberal-world-order-abiding governments prevail. If such countries instead succumb to constant gray-zone aggression, neither the countries nor the businesses based in them will thrive. Unlike Deutsche Bank during Schmidt's chancellorship, firms may not be patriotically minded and may, if asked, refuse to do a good deed for their home countries. Every company will, however, carry out an action that benefits the company itself. If governments can offer their private sectors opportunities for engagement that benefit both national security and the businesses themselves, many would likely participate. This would be even more likely if consumers, business customers, and the wider public rewarded businesses for helping the country. In light of the rapidly growing distrust of China among Western citizens,[68] Western brands cooperating with China may soon suffer in the court of public opinion.

Government-Industry Leader Briefings. As with citizen engagement, such engagement could begin with a basic form of participation: regular consultations between business leaders and top government officials. Today, businesses receive, from consultancies and other private-sector services, regular updates on unrest, kidnap risks, and similar developments that can affect their operations. While this allows them to evaluate such tactical risks, they are on much less sure footing in strategic developments. Such strategic assessments have long been governments' domain. This has led to a situation in which, as Finnish executive Risto Penttilä notes, "executives today would rather listen to [Jim] Mattis than to the global head of McKinsey & Co."[69]

Regular consultations with key government officials would address executives' desire to better understand the changing geopolitical context in which their companies operate. The briefings would be off-the-record, unclassified, and available to invited top executives in all sectors. Government officials would share national security updates and discuss the context of these events, though the briefings would naturally not feature any details that could give participants commercial advantages. Instead, they would provide the overall picture of international developments that business leaders currently lack.

The objective would clearly not be to pressure business leaders toward particular actions—which would be questionable in a liberal democracy—but to help inform their decision-making. This way, executives would at least be aware of the nation's

interests when making commercial decisions. For governments, the briefings would also be an opportunity to hear business leaders' accounts of the changing national security environment and help government decision makers understand what companies can and cannot do. The briefings would thus strengthen existing relationships between business leaders and the government and help business leaders understand their role in national resilience while giving top government officials a better understanding of the businesses' experiences in the geopolitical line of fire.

The briefing invitees could also include entertainment executives, academic leaders, religious leaders, and other civil society leaders such as heads of NGOs and arts institutions. Not least because of the disinformation in harming Western societies, the briefings should of course also involve social media executives.

Government-industry briefings, of course, do not preclude regulation. In the social media sector, Damian Collins—a Conservative member of the UK Parliament and former chair of its Committee on Digital, Culture, Media and Sport—argued that regulation is necessary.

> We need a regulatory code for social media platforms, led by an agency like Ofcom. There also need to be independent bodies that can set standards. Banks can't launch new products without FCA [Financial Conduct Authority] approval. And if a bank fails to spot certain conduct, they can be fined. There should be something like Know Your Customer for social media platforms.[70]

Regardless of whether social media regulators are established in the short term, keeping leaders in all societal and business sectors informed of new gray-zone developments would benefit their understanding of the situation. While such leaders may be aware of activities touching their own entities, they cannot be expected to be familiar with the entirety of gray-zone aggression at any given time and may thus be unable to put the activities intersecting with their own organizations into context.

Government-industry briefings would also be beneficial beyond exchanges of information. In isolation, organizations feel ill-equipped to identify, let alone address, interference and malign influence. Studio executives may, for example, be fully aware of the pressure to make films that have the best chances of pleasing Chinese censors but may not be familiar with the full extent of Chinese gray-zone aggression directed against Western countries. While governments of liberal democracies clearly cannot instruct the entertainment industry how to create its entertainment content, they can keep it informed of the wider picture of malicious activities by hostile states.

The US government operates a small version of the proposed government-industry briefing program focused on cyber threats. Maj. Gen. Ed Wilson (ret.), who served as deputy assistant secretary of defense for cyber policy in the Donald Trump administration, pointed out that

> for the past few years we [the Department of Defense] have been inviting CEOs and COOs [chief operating officers] to events co-hosted by, together with the DOE [Department of Energy], with DHS [Department of Homeland Security] participation. The purpose is simply to tell them about the threats we're seeing. We've also laid out sensors in cooperation with industry. A regional utility can't go toe to toe with Russia or China. DHS and Treasury have similar meetings. We want business leaders to understand the risk cyber aggression poses to their companies. Large companies have teams that can evaluate threats but smaller ones don't.[71]

The DOE explains that it works "to develop technologies, tools, exercises, and other resources to assist the energy sector in evaluating and improving their security posture, practices, and readiness."[72] As with the proposed national security consultations, the meetings form a "bi-directional sharing" of cyber threat information.[73] In Britain, the National Cyber Security Centre[74] exchanges information with key sectors and occasionally arranges meetings for top executives.

Artistic Side Benefits of National Security Awareness. In entertainment, consultations could yield a side benefit that may seem trivial but could have significant impact. To date, a smaller number of movies and TV drama series have featured gray-zone aggression-like story lines. The Norwegian hit series *Occupied* portrays a subversive attack on Norway that begins when a global energy crisis combined with climate change convince the country's prime minister to switch off its fossil-fuel production. His actions prompt gray-zone attacks by both the EU and Russia. Steven Soderbergh's 2011 movie *Contagion*[75] features a pandemic of the kind that became reality with COVID-19. With its subversive features that can be found in random parts of everyday life, the gray zone lends itself to outstanding entertainment content, but filmmakers and entertainment executives currently lack insights into it. Through participation in government briefings, they could not only learn about how gray-zone aggression affects their own sector but also, as a side benefit, get inspiration for new productions.

Indeed, entertainment content forms another way in which liberal democracies can strengthen resilience against gray-zone aggression. Millions of people on different continents have already watched *Occupied*[76] or *Contagion* because the shows are outstanding entertainment. Neither *Occupied* nor *Contagion* was initiated by a government; indeed, government meddling harms the quality of content. Yet entertainment ideas resulting from government-industry gray-zone briefings—which could range from feature films to TV drama series to reality shows similar to Sweden's *Blacked-Out Country* (*Nedsläckt land*), which follows a group of people during an extended power cut[77]—could not only provide compelling entertainment but also raise public awareness of vital national security issues. To date, *Occupied*, in fact, may well be most ordinary citizens' main source of information about gray-zone aggression.

Public Awareness and Corporate Behavior. Awareness of Beijing's pressure on the Western film studios in particular is growing among the Western public. As recent Pew Research Center polling on global public opinion of China demonstrates, so is distrust of China.[78] As a result, close involvement with China poses a reputational risk to Western companies, similar to what was the case with South Africa's apartheid regime. In the face of public pressure at home, many Western companies and institutional investors rescinded dealings with South Africa. While globalization has created a culture in which Western firms cooperate with authoritarian regimes for the sake of market access even as they shun committing to national efforts in their home countries, this model may no longer be viable. Indeed, close cooperation with authoritarian regimes may begin to backfire on Western firms.[79]

Disney's high-profile action drama *Mulan* is a case in point. Almost as soon as it was released in 2020, *Mulan*, which was considered a prospective blockbuster that could please the Chinese market, was greeted with enormous criticism. In posts that rapidly spread on social media, often using the hashtag #BoycottMulan, detractors pointed out that not only had the filming partially taken place in Xinjiang—where the Chinese government oppresses a minority—but also Disney, in the closing credits, even thanked authorities involved in the operation of Uyghur "reeducation" camps.[80] Instead of generating headlines for any artistic merits or box office success, *Mulan* generated controversy for Disney.

Joint Military-Industry Gray-Zone Exercises. A more comprehensive part in private-sector engagement is joint military-industry gray-zone exercises, a step proposed in a September 2020 paper[81] and pioneered by the Czech Republic soon afterward.[82] While most businesses conduct crisis management exercises, such exercises concern tactical threats such as terrorist attacks or kidnappings of their staff. Because gray-zone aggression is not directed against specific companies but affects them because they happen to be based in a particular country or because they are targets of convenience, it is virtually impossible for businesses to exercise for gray-zone threats on their own. Yet precisely because liberal democracies' private sectors cannot deflect such aggression, they are vulnerable targets.

Armed forces, in turn, constantly exercise but focus on threats involving sustained use of force by adversaries. They lack the capacity to defend the private sector against gray-zone threats, and doing so is at any rate not their focus. It is clearly in countries' interest that their private sectors not—unwittingly—provide adversaries with opportunities for gray-zone aggression, and equally it is in businesses' interest to minimize the effect of gray-zone aggression on their operations. Joint military-industry gray-zone exercises would be led by the armed forces and include selected businesses and security-related government agencies such as the police. Some businesses would be identified and invited by the government based on their strategic importance for the country, while others would participate following an application procedure. Exercises would include only a small tabletop component and instead primarily feature computer-simulated scenarios, which would regularly be updated to reflect the gray-zone threats.

Unlike existing corporate crisis management exercises, which are often only attended by employees responsible for a firm's crisis management and are at any rate tabletop exercises, the gray-zone exercises' different segments would involve representatives from all levels of a business, reflecting armed forces' exercise model. They would, of course, also involve government agencies with crisis responsibilities and senior political decision makers.

Firms completing the exercise would be granted an ISO 9000-style certification, which could be kept current through recurring participation. Such certification would signal to shareholders that the company belongs to an elite class of companies in resilience and that shareholders can therefore have a high degree of confidence the firm will emerge from national and international contingencies with only limited damage. Considering the reputational, monetary, and stock-price damage suffered by businesses successfully targeted by gray-zone attacks, such certification would likely become a considerable asset and could become a feature of corporate annual reports in much the same way as corporate social responsibility.

Like all national security exercises, joint military-industry gray-zone exercises also signal to adversaries that aggression will not yield the hoped-for results. As the UK Ministry of Defence's Development, Concepts and Doctrine Centre notes, "An actor that repeatedly carries out actions that contribute to deterrence will build their credibility, both with those who are a direct recipient of their action and other observers."[83]

The Czech exercise initially involved the country's five largest defense companies, with further iterations to include energy, IT, health care, and food production. "We see industrial policy as part of not only economic welfare, but geopolitics and also defence and security," Deputy Minister of Defense Tomáš Kopečný told the *Financial Times*.

> This exercise is basically about creating [a] nexus between the military and civilian, between the government and private side. . . . The very strategy that is being applied by Chinese state-affiliated investors is something that is targeting [Europe's] critical and strategic technologies. . . . It's definitely something that is decreasing our capability to defend ourselves, through us losing our technologies that are essential for defence.[84]

National Security Courses. Finnish-style national security courses represent a similarly ambitious option.[85] As in Finland, such a course would be an opportunity for employers in all parts of society to nominate promising mid-career leaders for national security education that also connects them with other leaders. For any country, it is invaluable when the top echelon in society—from members of parliament to heads of NGOs—mostly shares a basic understanding of national security and knows one another. This, too, contributes to creating a combined shield that signals to adversaries that a society is united in wanting to protect itself.

Finland's national defense course expressly does not aim to create a military-industrial complex; on the contrary, that only 6 percent of the participants come from the armed forces—compared to 32 percent from the commercial sector; 19 percent from media, NGOs, and labor market organizations; and 12 percent from academia[86]—highlights the course's civilian nature.

Such a focus should also be the goal of prospective future national security courses. As with the Finnish course, the aim should clearly be to inform the participants about the country's national security background and current situation, not to try to influence any political convictions they may hold.

Business Leader Allegiance. All three prospective forms of private-sector involvement proposed above—government-industry briefings, military-industry gray-zone exercises, and national security courses—are based on the assumption that private-sector and civil society leaders will feel at least rudimentary allegiance to the country in which they and their organizations are based. How does one reconcile this with globalization, which features not just top personnel of other nationalities but also foreign ownership even of iconic firms? For example, that Volvo is now owned by Geely of China[87] may invalidate the old saying that "what is good for Volvo is good for Sweden."

It is difficult. While foreign executives may well feel an allegiance to their businesses' home country, it cannot be assumed they will. In the case of foreign-owned companies, the situation is even more challenging, as they have an obligation to consider their owners. If forced to choose, will such a business act in a way that favors its home government or its owner? The latter will likely win.

Yet it is in everyone's interest that liberal democracies continue to thrive. While they may have lost some of their innovation advantage—partially because of subversive economics—these countries remain the world's most desirable bases for businesses. They have rule of law, freedom from political interference in business activities, and highly educated and innovative populations. Indeed, having their headquarters in liberal democracies shields global businesses from the reach of the authoritarian governments whose interference they tolerate as the prize of operating in those governments' markets.

Turning the Cold War equation around, what is bad for the UK, Germany, Sweden, or the United States today is bad for the companies operating there. Indeed, because businesses are already targets of gray-zone aggression, they are painfully aware of the reality though not fully familiar with its extent. It is thus in business leaders' and businesses' interest to help keep their home countries safe.

Government-Owned Investment Funds. Considering the extent of subversive economics, an additional measure would contribute to the wall of denial: the creation of government-owned investment funds. In the 1970s, Schmidt could ask Deutsche Bank to buy a stake in Daimler-Benz as an act of patriotism. New legislation in many Western countries will, of course, require government approval for buyers from non-EU, non-NATO, and non–Five Eyes countries in more areas than has been the case to date, but bans resulting from such legislation raise a new question: If a Chinese or other foreign firm is turned down, who will buy the stake? Many businesses will need some sort of recompense for not being allowed to accept a foreign investment. Solutions like the German government using its KfW bank to thwart a Chinese stake in a crucial energy provider are only patchwork solutions, as are direct government takeovers such as the UK government's bailout of Royal Bank of Scotland, one of the country's largest banks, in 2008.[88]

As a first step, governments could strengthen today's rudimentary cooperation with private-sector investors. It would be based not on patriotic pleas but on business opportunity. Foreign investors are interested in cutting-edge Western firms for their business potential (sometimes in combination with their national security utility). Through regular contact with private-sector investors, governments could steer investors' interest in the direction of businesses whose foreign offers it has blocked. This should obviously be done transparently so that no investor gains exclusive information.

Governments could also get involved as investors in their own right. Considering that the businesses whose foreign investors are likely to be blocked by many countries' recent foreign direct investment legislation are considered essential to the national interest, it is in the government's interest to invest in them. Indeed, precisely because such firms are

vital to national security in the wider sense, government investments in them would not be a waste of taxpayer money. On the contrary, it could be a good investment. In June 2020, the European Commission published a white paper proposing an investment fund for this purpose,[89] though member states have not yet taken any concrete steps. Such investment funds would be a radical step for most Western governments that today take a highly hands-off approach to the private sector. Yet if the subversive economics aspect of globalization is to be minimized, something has to replace the subversive actors.

The same is true for venture capital (VC) investments. While US legislation now limits foreign VC investments by foreign nationals, many other Western countries lack such protection. Somewhat surprisingly, the US government is also more actively involved in the VC sector than any other Western government is, primarily through VC investors such as the CIA-affiliated In-Q-Tel[90] and the Army Venture Capital Initiative.[91] The Estonian government, in turn, owns the VC fund SmartCap,[92] while the UK government's National Security Strategic Investment Fund functions as a miniature In-Q-Tel.[93] In February 2021, the UK government also launched the Advanced Research and Innovation Agency, whose 800 million euro fund chest will fund high-risk innovation similar to how the United States' Defense Advanced Research Projects Agency does.[94]

Since In-Q-Tel's launch in 1999, its investments have benefited US national security and generated financial returns that In-Q-Tel has reinvested. The same scenario appears likely for any further government-established VC funds. Indeed, government-supported VC firms similar to In-Q-Tel would not just benefit the startup community and with it national innovation and the economy but also be a good use of taxpayer money. Crucially, such funds could also reduce the attraction not just of foreign VC funds but also of limited partners. This would, of course, be the case especially if startup entrepreneurs were conversant with the national security implications of accepting funding from VCs or limited partners with connections to regimes hostile to the West.

Conclusion: The Collective Benefit of Civil Society Participation

Gray-zone exercises alone will clearly not change an adversary's cost-benefit calculus. Nor will government investment funds, resilience training, national defense courses, public-awareness campaigns, or any of the other initiatives proposed above. Yet together, they can help create a wall of denial to help deter other practices including IP theft, disinformation, and cyberattacks. None of the initiatives imposes a heavy burden on citizens or businesses; on the contrary, participating may benefit them and the country. As a wall of denial is a purely defensive act, these measures would also unlikely escalate tension with the West's adversaries.

Apart from public-awareness campaigns and especially business leader consultations, which could be initiated quickly, creating convincing resilience as outlined above would take time. In addition, it would need to be created under the intense scrutiny of hostile states that would also likely test any new initiatives as they were being set up and possibly use them as fodder for disinformation and misinformation. The time required may, however, be shorter than expected: The Czech Republic launched its gray-zone exercise in less than three months after the publication of the report on which it is based. Pilot projects would be a practical way of acting relatively quickly, and through pilot projects, organizers can spot gaps at any early stage.

Another question is who would coordinate the efforts. This could be a resilience czar or, in larger countries, perhaps a group of resilience czars—respected leaders who could, not least through their personal standing in society, encourage participation. Seasoned former business leaders or civil society leaders would be well-suited for this role.[95]

Building resilience against an adversary whose government can simply command action is undoubtedly a vexing task, but it is a key answer to helping keep liberal democracies safe. Voluntary participation in helping keep the country safe is, of course, what made Sweden's and Finland's Cold War total defense convincing even as they faced similar

obstacles. With voluntary and multifaceted civil society participation, liberal democracies can reduce the gray-zone opportunities for their adversaries, who may continue to possess intent and capability but whose ambitions will be thwarted if their opportunities are reduced.

Western countries should naturally also try to negotiate international gray-zone norms with their adversaries, but with societal resilience in place, they will be equipped to create a wall of denial against gray-zone aggression.

About the Author

Elisabeth Braw is a resident fellow at the American Enterprise Institute, where she focuses on defense against emerging national security challenges, such as hybrid and gray-zone threats. She is also a columnist with *Foreign Policy*, where she writes on national security and the globalized economy, and a member of the UK's National Preparedness Commission.

Acknowledgments

I would like to thank Chris Brannigan, Ewan Lawson, Lord George Robertson KT GCMG PC, and Brig. Gen. Gerhard Wheeler CBE (ret.) for their input on this report.

Notes

1. Klara Obermüller, ed., "Wir sind eigenartig, ohne Zweifel. Die kritischen Texte von Schweizer Schriftstellern über ihr Land" [We're peculiar, without a doubt. Critical text by Swiss authors about their country], Nagel & Kimche, https://files.hanser.de/Files/Article/ARTK_LPR_9783312003174_0001.pdf.
2. North Atlantic Treaty Organization, "North Atlantic Treaty," April 4, 1949, https://www.nato.int/cps/en/natolive/official_texts_17120.htm.
3. Other countries, notably Norway and Denmark, built similar systems. Sweden's and Finland's approach is, however, selected here as a basis for learning.
4. Wolf-Diether Roepke and Hasit Thankey, "Resilience: The First Line of Defence," NATO Review, February 27, 2019, https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html.
5. Roepke and Thankey, "Resilience."
6. Elisabeth Braw, "Producing Fear in the Enemy's Mind: How to Adapt Cold War Deterrence for Gray-Zone Aggression," American Enterprise Institute, March 9, 2021, https://www.aei.org/research-products/report/producing-fear-in-the-enemys-mind-how-to-adapt-cold-war-deterrence-for-gray-zone-aggression/; and Elisabeth Braw, "The Defender's Dilemma: Defining, Identifying, and Deterring Gray-Zone Aggression," American Enterprise Institute, February 8, 2021, https://www.aei.org/research-products/report/the-defenders-dilemma-defining-identifying-and-deterring-gray-zone-aggression/.
7. Lyle J. Morris et al., "Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War," RAND Corporation, 2019, 140, https://www.rand.org/pubs/research_reports/RR2942.html.
8. Niklas Karlsson (Social Democratic member, Swedish parliament), telephone interview with the author, August 11, 2020.
9. HM Government, UK Cabinet Office, *National Security Capability Review*, March 2018, 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf.
10. HM Government, UK Cabinet Office, *National Security Capability Review*, 11.
11. UK Civil Defence Association, "Brief History of UK Civil Defence," https://civildefenceassociation.uk/history/.
12. Ole Wæver et al., *Identity, Migration and the New Security Agenda in Europe* (New York: St. Martin's Press, 1993), 23.
13. HM Government, *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*, March 2021, 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/969402/The_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf.
14. HM Government, *Global Britain in a Competitive Age*, 88.
15. HM Government, *Global Britain in a Competitive Age*, 99.
16. Carl Rådestad and Oscar Larsson, "Responsibilization in Contemporary Swedish Crisis Management: Expanding 'Bare Life' Bio-politics Through Exceptionalism and Neoliberal Governmentality," *Critical Policy Studies* 14, no. 1 (October 9, 2018): 92, https://www.tandfonline.com/doi/full/10.1080/19460171.2018.1530604?af=R.
17. Federal Government of Germany, *White Paper on German Security Policy and the Future of the Bundeswehr,* 2016, 39, https://www.gmfus.org/publications/white-paper-german-security-policy-and-future-bundeswehr.
18. Rådestad and Larsson, "Responsibilization in Contemporary Swedish Crisis Management," 39.
19. Elisabeth Braw, *Competitive National Service: How the Scandinavian Model Can Be Adapted by the UK,* Royal United Services Institute for Defence and Security Studies, October 23, 2019, https://rusi.org/publication/occasional-papers/competitive-national-service-how-scandinavian-model-can-be-adapted-uk.
20. KAVI, *Finnish Media Education: Promoting Media and Information Literacy in Finland*, https://kavi.fi/sites/default/files/documents/mil_in_finland.pdf.
21. Government of Finland, Security Committee, *Security Strategy for Society*, 2018, 5, https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf.

22. Government of Finland, Security Committee, *Security Strategy for Society*, 7–8.

23. Regeringskansliet, *Inrättande av Myndigheten för psykologiskt försvar* [*Establishment of the Agency for Psychological Defense*], March 18, 2021, https://www.regeringen.se/rattsliga-dokument/kommittedirektiv/2021/03/dir.-202120/.

24. Gerhard Wheeler, "Northern Composure: Initial Observations from Sweden's Total Defence 2020 Exercise," Royal United Services Institute for Defence and Security Studies, September 3, 2020, https://rusi.org/commentary/northern-composure-initial-observations-swedens-total-defence-2020-exercise.

25. Government of Denmark, *Foreign and Security Policy Strategy, 2017–2018*, June 14, 2017, https://www.regeringen.dk/publikationer-og-aftaletekster/udenrigs-og-sikkerhedspolitisk-strategi-for-2017-2018/.

26. Republic of Estonia, Ministry of Defence, *National Security Concept 2017*, 8, https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017_0.pdf.

27. Kaitselit, "Estonian Defence League's Cyber Unit," https://www.kaitseliit.ee/en/cyber-unit.

28. Elisabeth Braw, "How We Can Tackle the Next Invisible Enemy," *Times*, April 14, 2020, https://www.thetimes.co.uk/article/how-we-can-tackle-the-next-invisible-enemy-flqqpzww6.

29. Artis Pabriks, *How Latvia Accomplishes Comprehensive Defence*, Royal United Services Institute for Defence and Security Studies, June 25, 2020, https://rusi.org/commentary/how-latvia-accomplishes-comprehensive-defence.

30. Pabriks, *How Latvia Accomplishes Comprehensive Defence*.

31. Peter Singer and August Cole, *A Warning from Tomorrow*, US Cyberspace Solarium Commission, March 2020, 5, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

32. Lucy Williamson, "France's Raw Recruits Sign Up for Return of National Service," BBC, June 25, 2019, https://www.bbc.co.uk/news/world-europe-48755605.

33. Elisabeth Braw, "Ask What You Can Do for Your Country," *Foreign Policy*, August 4, 2020, https://foreignpolicy.com/2020/08/04/national-service-germany-usa-ask-what-you-can-do-for-your-country/.

34. Guna Gavrilko (head of the structure and military personnel development planning section, Latvian Ministry of Defense), in discussion with the author, summer 2020; and Ilze Leimane (head of the planning section of the cadet force of Latvia, Latvian Ministry of Defense), in discussion with the author, summer 2020.

35. For further information about this incident, see Gordon H. McCormick, "Stranger Than Fiction: Soviet Submarine Operations in Swedish Waters," Project Air Force, January 1990, 4–9, https://apps.dtic.mil/dtic/tr/fulltext/u2/a238953.pdf.

36. Ojars Kalnins (New Unity party member, Latvian parliament), in discussion with the author, June 25, 2020.

37. Monika Garbačiauskaitė-Budrienė (CEO, Lithuanian Radio and Television), in discussion with the author, January 15, 2020.

38. Monika Garbačiauskaitė-Budrienė, interview.

39. I outlined this proposal in Elisabeth Braw, "Citizen Alienation and the Political and Media Elite," University of Oxford, Reuters Institute for the Study of Journalism, August 2014, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-01/Citizen%20alienation%20and%20the%20political%20and%20media%20elite.pdf.

40. Tokyo Metropolitan Government, *Disaster Prevention Information*, https://www.metro.tokyo.lg.jp/english/guide/bosai/index.html.

41. SF72, "Earthquake," https://www.sf72.org/hazard/earthquake.

42. Kieran Dent and Ben Westwood, "Stress Testing of Banks: An Introduction," *Bank of England Quarterly Bulletin* Q3 (2016), https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2016/stress-testing-of-banks-an-introduction.pdf.

43. Elisabeth Braw, "We Must Learn What to Do If the Lights Go Out," *Times*, May 10, 2019, https://www.thetimes.co.uk/article/we-must-learn-what-to-do-if-the-lights-go-out-xlcph6cqt.

44. See, for example, ShakeOut, website, https://www.shakeout.org/.

45. Phil Helsel and Yuliya Talmazan, "Texas Water Shortage Adds to Power Crisis as New Winter Storm Moves in," NBC News, February 18, 2021, https://www.nbcnews.com/news/us-news/texas-contending-water-nightmare-top-power-crisis-n1258208.

46. BBC, "Russian Trolls' Chief Target Was 'Black US Voters' in 2016," October 9, 2019, https://www.bbc.co.uk/news/technology-49987657.

47. Kevin Roose, "What Is QAnon, the Viral Pro-Trump Conspiracy Theory?," *New York Times*, February 4, 2021, https://www.nytimes.com/article/what-is-qanon.html.

48. Ewan Somerville, "750,000 People Sign Up to Join NHS Volunteer Army in Less Than a Week," *Evening Standard,* March 29, 2020, https://www.standard.co.uk/news/health/coronavirus-nhs-army-applications-royal-voluntary-service-a4400821.html.

49. Technisches Hilfswerk, "Overview," https://www.thw.de/EN/THW/Overview/overview_node.html.

50. Student Volunteer Army, website, https://sva.org.nz/.

51. Singapore Civil Defence Force, "What Is Total Defence," https://www.scdf.gov.sg/home/community-volunteers/community-preparedness/total-defence.

52. Robert D. Putnam, *Bowling Alone: The Collapse and Revival of American Community* (New York: Simon and Schuster, 2000).

53. UK Office for National Statistics, "Families and Households in the UK: 2019," November 15, 2019,https://www.ons.gov.uk/peoplepopulationandcommunity/birthsdeathsandmarriages/families/bulletins/familiesandhouseholds/2019.

54. Braw, *Competitive National Service*.

55. Lithuania has selective national service, though it admits a higher percentage than Denmark, Norway, and Sweden do.

56. Norwegian Armed Forces, *Årsrapport 2019* [*Annual Report 2019*], 2019, https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/forsvarets-arsrapport/Forsvaret-aarsrapport2019_web.pdf/_/attachment/inline/7cd7c737-ddad-4ac3-a97f-742b9dc6d6e3:ebcecbe81a552443e801808d49391bbab240e570/Forsvaret-aarsrapport2019_web.pdf.

57. Statisics Norway, "Fakta om befolkningen" [Facts about the population], https://www.ssb.no/befolkning/faktaside/befolkningen.

58. Information provided to the author by the Norwegian Armed Forces.

59. Universum, "The Most Attractive Employers in Norway: Students 2020," 2020, https://universumglobal.com/rankings/norway/.

60. See Norwegian Armed Forces, "Cyberværneplikt" [Cyber Defense], https://karriere.forsvaret.dk/varnepligt/varnepligten/cybervarnepligt/; and Swedish Armed Forces, "Försvarsmakten utbildar cybersoldater" [The Armed Forces trains cyber soliders], February 15, 2019, https://www.forsvarsmakten.se/sv/aktuellt/2019/02/forsvarsmakten-utbildar-cybersoldater/.

61. As previously noted, China's personal protective equipment deliveries during the first COVID-19 wave were modest and contained a significant amount of faulty products. In addition, the recipient countries had in many cases purchased a large share of the goods, making it a commercial arrangement rather than assistance.

62. Ellen Terrell, "When a Quote Is Not (Exactly) a Quote: General Motors," Library of Congress, April 22, 2016, https://blogs.loc.gov/inside_adams/2016/04/when-a-quote-is-not-exactly-a-quote-general-motors/.

63. Phoenix, "Helmut Schmidt im Gespräch mit Ulrich Wickert" [Helmut Schmidt in conversation with Ulrich Wickert], YouTube, November 26, 2016, https://www.youtube.com/watch?v=i18VPjFcsLQ&t=1137s.

64. Phoenix, "Helmut Schmidt im Gespräch mit Ulrich Wickert" [Helmut Schmidt in conversation with Ulrich Wickert].

65. McDonald's, "Our Leadership," https://corporate.mcdonalds.com/corpmcd/our-company/who-we-are/our-leadership.html.

66. Elisabeth Braw, "Will American Firms Put America First?," *Foreign Policy*, February 21, 2020, https://foreignpolicy.com/2020/02/21/davos-wef-will-american-companies-put-america-first/.

67. Daimler, "Ola Källenius, Chairman of the Board of Management of Daimler AG and Mercedes-Benz AG," https://www.daimler.com/company/corporate-governance/board-of-management/kaellenius/.

68. Laura Silver, Kat Devlin, and Christine Huang, "Unfavorable Views of China Reach Historic Highs in Many Countries," Pew Research Center, October 6, 2020, https://www.pewresearch.org/global/2020/10/06/unfavorable-views-of-china-reach-historic-highs-in-many-countries/.

69. Elisabeth Braw, "Military Knowhow Can Help Business Navigate a Hostile World," *Financial Times,* March 21, 2021, https://www.ft.com/content/91768471-f991-40ef-a976-448568600b0f.

70. Damian Collins (Conservative Party member, UK Parliament), in discussion with the author, June 8, 2021.

71. Ed Wilson (former deputy assistant secretary of defense for cyber policy, US Department of Defense), in discussion with the author, June 25, 2020.

72. US Department of Energy, "Energy Sector Cybersecurity Preparedness," https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity.

73. US Department of Energy, "Energy Sector Cybersecurity Preparedness."
74. National Cyber Security Center, website, https://www.ncsc.gov.uk/.
75. Steven Soderbergh, dir., *Contagion* (Hollywood, CA: Warner Bros. Pictures, 2011).
76. Karianne Lund, Jo Nesbø, and Erik Skjoldbjærg, dirs., *Occupied* (Sweden: Yellow Bird, 2015).
77. Björn Östlund, dir., *Nedsläckt land* [*Blacked-Out Country*] (Sweden, 2019).
78. Silver, Devlin, and Huang, *Unfavorable Views of China Reach Historic Highs in Many Countries*.
79. Elisabeth Braw, "Why Western Companies Should Leave China," *Foreign Policy*, February 17, 2021, https://foreignpolicy.com/2021/02/17/why-western-companies-should-leave-china/.
80. Ryan Faughnder and Alice Su, "How Disney's 'Mulan' Became One of 2020's Most Controversial Movies," *Los Angeles Times*, September 11, 2020, https://www.latimes.com/entertainment-arts/business/story/2020-09-11/disneys-mulan-debuts-in-china-heres-why-its-controversial.
81. Elisabeth Braw, "The Case for Joint Military–Industry Greyzone Exercises," Royal United Services Institute, September 28, 2020, https://rusi.org/publication/briefing-papers/joint-military-industry-greyzone-exercises.
82. Helen Warrell, "Czech Republic Turns to War-Games to Build Cyber Defences," *Financial Times*, February 18, 2021, https://www.ft.com/content/8c018644-3866-4f69-9105-d3c0e68ca491.
83. UK Ministry of Defence, Development, Concepts and Doctrine Centre, *Deterrence: The Defence Contribution, Joint Doctrine Note 1/19*, February 2019, 50, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/860499/20190204-doctrine_uk_deterrence_jdn_1_19.pdf.
84. Warrell, "Czech Republic Turns to War-Games to Build Cyber Defences."
85. Lithuania has a similar course, as does Sweden, the concept's originator.
86. The percentages were provided by Arto Räty (retired lieutenant general and former director, National Defense Course), in discussion with the author, April 12, 2019.
87. Reuters, "Geely to Deepen Ties with Volvo, Plans to List Under One Umbrella," February 10, 2020, https://www.reuters.com/article/us-volvo-cars-m-a-geely-automobile/geely-to-deepen-ties-with-volvo-plans-to-list-under-one-umbrella-idUSKBN2041D5.
88. Emma Rumney, "UK Government Plans to Sell Remaining RBS Stake by 2024," Reuters, October 29, 2018, https://www.reuters.com/article/uk-britain-economy-rbs/uk-government-plans-to-sell-remaining-rbs-stake-by-2024-idUKKCN1N32E7.
89. European Commission, "White Paper on Levelling the Playing Field as Regards Foreign Subsidies," June 17, 2020, https://ec.europa.eu/competition/international/overview/foreign_subsidies_white_paper.pdf.
90. In-Q-Tel, website, https://www.iqt.org/about-iqt/.
91. Army Venture Capital Initiative, website, http://armyvci.org/.
92. SmartCap, website, https://smartcap.ee/.
93. National Security Strategic Investment Fund, website, http://www.british-business-bank.co.uk/national-security-strategic-investment-fund/.
94. UK Government, Department for Business, Energy and Industrial Transformation, "UK to Launch New Research Agency to Support High Risk, High Reward Science," February 19, 2021, https://www.gov.uk/government/news/uk-to-launch-new-research-agency-to-support-high-risk-high-reward-science.
95. In the UK, the House of Lords offers an ideal selection of respected leaders from whom resilience czars could be selected.