Natural Hazards and National Security

The COVID-19 Lessons

By David Omand

Natural hazards can have serious implications for national security. The COVID-19 pandemic illustrates how first-order challenges are created for our national security planners, not least maintaining SSBN and SSN submarine crew and air crew rosters during quarantine restrictions, as well as keeping forces operationally effective while establishing social distancing in supply, repair and support facilities, gyms, and mess halls. We must also expect our adversaries to try to exploit the dislocation such events cause to further their own agendas.

From our painful experience of COVID-19, we can draw general lessons for planning against the potential impact on national security of a range of natural hazards. In this article, I also want to address some of the less direct second- and third-order effects of COVID-19 that have wider implications for our future national security.[1] Those indirect effects prompt the question of whether we have adequately defined the boundaries of what ought to be included within the rubric of planning for national security in the future. That in turn raises the question of where the balance of argument lies in moving in the direction of a Scandinavian-style "total defense" against both threats and natural hazards. That would likely involve some extension of the scope of the funded missions of the armed forces, and enlargement of the responsibilities of defense departments over an expanding national security space. There are important debates to be had drawing on the lessons from the COVID-19 experience, from how best to organize national resources for an all-of-nation response and identifying and analyzing potential natural hazards, to making informed choices as to where best to invest in precautionary measures that will meet with public support.

Threats and Hazards

In this article I am using the term *threat* to refer to security challenges that have human agency behind them, whether from state or non-state actors; and the term *hazard* to refer to the impersonal forces of nature that can create disruptive challenges, ranging from naturally occurring infectious disease to coronal ejections of damaging charged particles from the sun.

Professor Sir David Omand is a Visiting Professor at the War Studies Department at King's College London and the former UK Security and Intelligence Coordinator and Director, GCHQ.

British governments have traditionally preferred to use the term "disruptive challenge," rather than crisis to describe the arrival of such events, since the essence of what makes a crisis is events that succeed each other so fast that the normal processes of decision-making cannot keep pace. Governments do not like to give the impression they have lost control—that may lead them into overly optimistic pronouncements of how they are managing disruptive situations. I will therefore in this article reserve the word "crisis" for when I am anticipating precisely that temporary loss of control due to the pace of events.

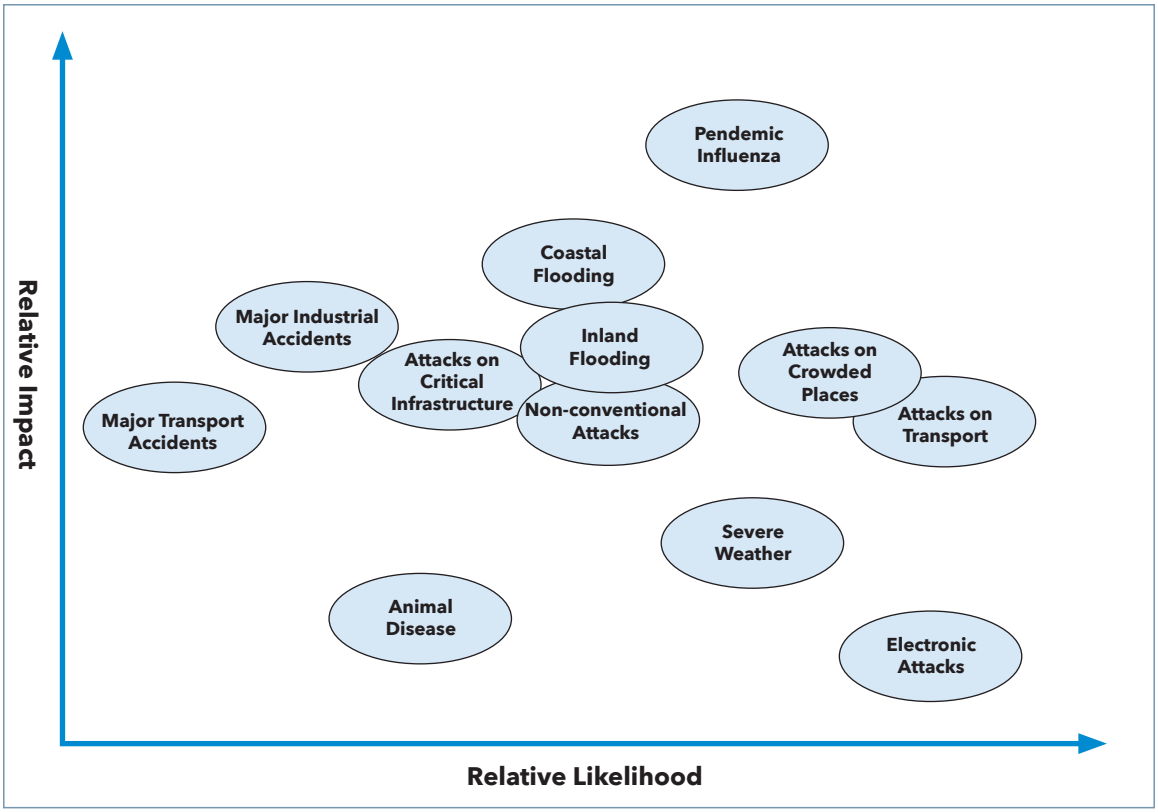
These categories of threat and hazard can interact of course. Disease can be spread maliciously, refugee movements from drought-affected areas can create security issues, unlawful human destruction of rainforests accentuates global warming, and so on. The essence of the important distinction for contingency planners lies in the impersonality of natural forces in contrast to the ability of malign actors to learn from experience and adjust their threat vectors so as to defeat countermeasures. Even so, we should not forget that hazards can change, too—viruses can mutate, and infections develop resistance to antibiotics.

Threats have so far been the dominant category for consideration in national security planning. Policymakers and planners in both the United States and UK national security communities have been preoccupied over the past decade with the resurgence of serious threats from potentially hostile nation states, continuing instability in the Middle East, threats from Salafist jihadist terrorists, and most recently from a wave of damaging cyber espionage and destructive malware and ransomware, not to mention digital subversion coming from Russia seeking to interfere in our democratic processes. The financial losses from malicious cyber activity have also become a matter of significant concern. The NotPetya malware, for example, that the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (also known as the GRU) deployed to try to digitally coerce targeted Ukrainian enterprises, ended up escaping into the wild and doing $10 billion worth of damage to global private companies, a very significant sum.

Yet the likely financial and social impact of such threats pales in significance compared to the speed and depth of the effects of the COVID-19 pandemic. The coronavirus caused a contraction in U.S. gross domestic product at the fastest rate ever recorded between April and June 2020.[2] The UK is in its deepest recession in at least a century.[3] The pandemic has done more economic damage and social dislocation, resulting in the premature deaths of more people, than any hostile terrorist or cyberattack could have.

Apart from these damaging direct effects, the medium-term consequences for defense budgets could be severe as tax receipts shrink and public expenditure is squeezed.[4] If interest rates rise over the next decade, the reductions in public expenditure in NATO nations could be extreme in order to pay the interest on national debt wracked up to provide for necessary short-term economic and social relief from the immediate effect of the virus, as well as to stimulate recovery. The slowdown in global economic activity will heighten these dangers.

A coronavirus pandemic is just one of the many types of major disruptive hazards we must expect from nature. Since 2008, the British government has annually published a National Risk Register[5] to describe the key risks that have the potential to impact the British population. The Register includes risk matrices showing the most serious risks plotted against measures of likelihood and impact. Since 2008, those matrices have all featured a pandemic caused by a mutated influenza virus located in the top right-hand corner of the diagram as being the most concerning in terms of a combination of likelihood of the outbreak occurring with the impact to be expected. These take into account the vulnerability of the population to a new respiratory disease



Matrix A -Hazards, diseases, accidents, and societal risks and Matrix B -Malicious attack risks (UK Cabinet Office, 2017)

that would be markedly different from past influenza viruses and to which few people, if any, would have immunity. Other risks of concern shown in the UK matrix include the threat of terrorist attacks on transport systems and in crowded places, as well as cyberattacks, but in those cases showing a less concerning combination of probability and impact (their "expected value" in statistical terms).

There are many natural hazards that could have a damaging impact on our societies including other human diseases such as Ebola; animal pathogens that affect humans such as West Nile virus; space weather events such as coronal mass ejections and solar flares that impact electronics; and major environmental events, including volcanic eruptions, earthquakes, and tsunami. There are also trends in global climate change that appear to show a greater occurrence of extreme weather events including hurricanes and tornadoes, large-scale cold spells and flooding, and long-lasting heatwaves. Sea level rises are predicted that, combined with storm surges, will displace large numbers of people by mid-century and increase refugee flows.

The Impact on National Security Missions

It is an important responsibility of government to ensure that well-trained people and systems are available to identify and plan ahead to mitigate the impact of such major hazards. We must expect our adversaries will look for ways to capitalize on any misfortunes that may befall us as a result of natural hazards. Disruptions to the functions of normal life,

such as we have experienced due to COVID-19, will allow malign actors greater opportunities to cause us trouble. We may consider that hitting a man when he is down or distracted is unsportsmanlike, but that is what our adversaries do. The COVID-19 experience should remind national security planners working with local, state, and national government officials, and health and social care professionals to take the future impact of major natural hazards seriously in their forecasts. COVID-19 reminds us all of the value of early intervention when a natural disaster strikes, and to think in advance of the value of contingency plans, stockpiles of key items, and some prior investment in system resilience, in mitigating the situation then faced.

Existing threats can themselves be amplified by the impact of hazards. As a result of COVID-19, we have seen a rise in opportunistic criminal cyberattacks, preying on a population that is working from home and ever more dependent on social media.[6] Terrorists may take advantage of temporary difficulties in the way that border control can be exercised during periods of disruption. The distraction of senior Western leadership during a crisis may offer opportunistic possibilities for adventurism between rivalrous states and non-state groups.

Many defense supply chains and several parts of the infrastructure serving defense commands have been disrupted by the restrictions imposed by national or regional COVID-19 lockdowns. We have known for decades that our modern logistics and repair capability rests precariously on the rapid availability of goods and services provided by many layers of contractors and component suppliers, not all of whom may be visible to the prime contractor supporting an equipment program, defense base, or other facility. It is easy to demand that supply chains be secured, but I recall that an early lesson in how hard this can be came for the UK in 2000 when there was serious disruption of gasoline distribution from oil refineries.[7] It proved impossible to separate out in advance which users "essential" to the working of the modern critical national infrastructure should be given priority supply. For example, a major teaching hospital ended up canceling complex operations, not because of its own fuel situation (it had emergency supplies under its contingency plans), but because modern surgical procedures use pre-prepared packs of sterilized instruments, which were delivered from a key contractor (who also was on the list for emergency access to fuel), but that contractor ran out of the sterilized shrink-wrap to protect the packs and the specialist company that supplied that material on a just-in-time basis had not been identified centrally as part of a supply chain needing protection from fuel disruption.

Supply chains run deep and, increasingly, overseas. The present COVID-19 pandemic has illustrated increasing dependence on globalized supply chains even in low-tech manufacturing, for example, personal protective equipment (PPE) such as protective clothing and masks. At least some of the fragility of defense supply chains comes from the seemingly relentless search by defense departments for greater efficiencies in supply and repair and support networks to free up defense resources for other priorities, as well as by defense contractors seeking to keep up profit rates for investors while under customer pressure to keep margins down. Low-cost sourcing overseas is superficially attractive in those circumstances. The greater availability of data from instrumenting platforms and systems, coupled with cheap computing and global communications, also makes it possible to engineer precise, just-in-time logistics systems that would not have been possible a decade ago. But if that is at the expense of resilience to unforeseen impacts on the system, it will prove a false economy when the unexpected happens. The COVID-19 experience should reinforce in the minds of law enforcement, defense, and security officials—and their contractors—the need to be aware of the increased risks to

MTA Deploys PPE Vending Machines Across Subway System (Metropolitian Transit Authority of the State of New York, June 29, 2020)

their ability to execute their missions that may arise when there are disruptive global challenges.

Both the U.S. and UK governments have horizon-scanning capability and deep scientific resources that can be engaged in establishing which possible events might have the most concerning combination of assessed likelihood and vulnerability in society. Whether such an event will crystalize into a significant risk depends both on the initial phase of impact and the duration of the ensuing disruption, itself dependent on societal resilience. How best to obtain systematic identification of those risks is considered later in this article.

Armed with risk matrices, governments and legislatures can then engage in a public debate about how reasonable it is to invest now in anticipatory measures to mitigate the effects of uncertain events in the future. There are tradeoffs to be made that must engage the political process since different types of risk will impact asymmetrically on different national interests and citizen groups. Decisions over long-term risks may involve weighing the interests of those alive today against those of future generations. Do we assume, for example, that future generations will be richer, as the economy develops, and thus more able—in welfare economics terms—to bear the burden of the costs associated with a long-term hazard? Such inter-generational tradeoffs are conventionally expressed in terms of a time rate of discount to be applied to the streams of costs and benefits from an investment to be expected over the period. The choice of that discount rate is a political choice and likely to be highly controversial, as we have already seen in arguments over how much to spend today to try to mitigate effects of climate change in the future.[8]

There are two more fundamental issues that surface, however, from the COVID-19 experience that are considered in the next two sections:

- The first is how far it would be sensible to bring together the national effort in relation to natural hazards with that designed to respond to malign threats from state and non-state actors. Should the definition of national security be expanded to cover both? Would there be an adverse public perception of "securitization" or of suspicions of unjustified mission creep by the military?
- The second is a consequence of the first; how then would it be best to organize to deliver all-of-nation protection for the public to deal with major hazards alongside the defense-driven response to traditional national security threats? In particular, how far should we alter the boundary of the missions that the intelligence community, armed forces, and defense departments have traditionally been assigned so that they can contribute better to defending us against extreme acts of nature as well as those of the nation's enemies?

The Scope of National Security

In the last 20 years (essentially, since the events of September 11, 2001), the United States and the UK have already been through a significant transition in the objectives of national security policy. The traditional national security missions remain; deterring potential adversary nations, having the ability to use military force to protect and promote the national interest, countering foreign espionage and sabotage, and generally defending the institutions of the state and upholding its constitutional values. The intelligence support for these missions preoccupied the agencies during the Cold War, including revealing the military capabilities of potential adversaries. To those defense-oriented objectives has been added the direct protection of citizens at home and overseas from the threats of international terrorism and serious organized crime, including cybercrime.

When British legislation[9] therefore refers to "national security" as being one of the legal justifications for the activities of the intelligence agencies and the use of intrusive powers, it is accepted that this includes countering terrorism and cyberattacks. The British Acts of Parliament also make explicit that the detection and prevention of serious crime is as proper a function of the national intelligence effort as it is for the armed forces at the request of the civil authorities; we see this today, for example, in the Royal Naval interdiction of narcotics trafficking in the Caribbean.[10] The intelligence community is putting significant effort into acquiring preemptive intelligence to support such activity and gathering information on malign actors as individuals; the hostile autocrats, dictators, terrorists, narcotics and human traffickers, cyber criminals, child abusers, and other international criminal gangs, all intent on doing things that will harm us. The urgent demands have been for intelligence on their (often multiple and hidden) identities, associates, locations, movements, financing, and of course intentions.[11]

All that represents a natural transition from "the Secret State" of the Cold War to "the Protecting State" of today.[12] Given the risks to citizens and to our armed forces posed by major natural hazards it is a logical next step to see national security increasingly being recognized as having a public safety and health dimension.[13] The drivers here are both the direct adverse impact on defense and security missions and the indirect risks to the affected sectors and thus the continuation of normal life. The COVID-19 pandemic has acted as a catalyst in advancing this recognition.

At this point it would also be right to recognize that the COVID-19 experience shows that such global crises can generate unexpected challenges of their own for Western intelligence and security

agencies— preventing others from stealing COVID-19 vaccine secrets and from spreading damaging and deliberate disinformation.[14] The modern approach to national security that I have suggested therefore has to be broad in scope to cover major hazards as well as threats. And with the implication that in the future there will be a much wider range of potential major disruptive challenges that will need to be studied by national security planners.

The demands for precautionary investment will have to compete alongside the needs of the present to maintain effective national security capabilities. Historically, we have had conceptual national security upheavals before, when the traditional security domains of sea and land had to accommodate air, and then space, and now cyberspace, and in future, I suggest, at least some of the major risks of the natural world. Such readjustments are never easy.

A significant step was taken by U.S. President Barack Obama (not least in light of the rise in cyber threats to the United States and the earlier lessons learned from the experience of Hurricane Katrina under his predecessor) by bringing the Homeland Security Council and the President's Homeland Security Adviser together with the National Security Council and the National Security Adviser. In the UK comparable steps were taken and the UK now has the Prime Minister chairing a single National Security Committee of the Cabinet, supported by a single National Security Adviser, covering domestic as well as overseas risks. At the top therefore the formal structures are in place to balance the requirements of preparing to respond to serious natural hazards as well as threats.

The Importance of Trustworthy Authorities

Once it is accepted that the safety and security of the citizen from major risks of whatever kind forms part of national security thinking we have to recognize the additional dimension of public psychology that this brings. What would it mean for a nation like the UK to be in the happy position of enjoying a state of national security? My answer is, when there is trust on the part of the public that the risks from the major threats and hazards facing the nation are being sufficiently mitigated to enable normal life to continue, freely and with confidence.

Freely meaning the aim of normality is achieved without government having to impose extreme restrictions that go against the grain of the values, freedoms, and rights we enjoy as democratic nations, or take repressive measures outside the rule of law.

With confidence meaning that the key indicators of normal life are positive, despite the existence of risks to life and property. That means we should see high levels of economic activity, research and innovation, stable markets, inward investment, a willingness of the public to vote and exercise their democratic rights and to access crowded spaces, and use public transport, children in schools, and so on. As an example, we can see that the psychologically based national security test has been met in relation to the continuing serious domestic threat in the UK from jihadist terrorism. Despite some anguishing attacks, the UK is not a nation in fear of the terrorist.

But in relation to the COVID-19 pandemic we are in a state of national insecurity. Confidence in government to take optimum decisions in a timely manner has been badly shaken on both sides of the Atlantic. All the confidence indicators I mentioned above are blinking red.

A significant lesson in statecraft to be learned from the present experience of COVID-19 events is about the value of government and its institutions firmly banking in quiet times a reputation for trustworthiness. Trustworthiness comes from observed, reliable, consistent, and truthful behavior, and keeping one's word. Faced with a common danger we should expect divisions in society to lessen and for local communities to come together, but we cannot count on quickly building up trust in the actions of

Flyers at Hartsfield-Jackson Atlanta International Airport wearing facemasks on March 6th, 2020 as the COVID-19 coronavirus spreads throughout the United States. (Chad Davis, March 6, 2020)

government itself in the midst of the inevitable confusion *after* a crisis has arrived. It is in those adverse circumstances that it really matters that the public already believes in the integrity and good intentions of a government and will follow its advice.

The Boundary of the Missions of the Armed Forces and Defense Departments

When a serious disruptive challenge arises, perhaps it will be one of the overlooked "grey rhinos" of the future;[15] we will look to our civil authorities to lead the response and the police services for domestic protection. But when civil resources become exhausted or falter, as has happened at times over the COVID-19 crisis, then governments have only one direction in which to look for relief—that is to seek the use of defense capability. That comes with the proven advantages of a reliable chain of command, experienced planners, resilient communications, and disciplined personnel. For most nations, those capabilities represent the last line of defense for the protection of the public. That is certainly the case in the UK. Polls consistently show high levels of public trust in the armed forces. And the British public has never been let down in that respect, as the highly successful use of the armed services to help deliver a safe and secure London Olympic Games in 2012 demonstrated—once, that is, the arguments about who should pay have been set aside.

That last observation has strategic implications for what governments regard as legitimate military tasks for which defense budgets should be properly funded and contingent financial provision made. Tasks that government accepts would have to be met on an opportunity basis by whatever capabilities happen to be available at the time with costs reimbursed by the Treasury or the relevant civil department.

Difficult judgments then have to be made over the relative priority that defense planners should be asked to give to the totality of approved missions and tasks. For the UK specifically, it may be coming to the point where "home defense" has to be re-thought in a context of total all-of-government protection against

the full range of threats and hazards, to create what I described as "the Protecting State." "Total defense" is a concept that has come back into prominence in Scandinavia and has lessons for other NATO nations.[16] A recent (August 2020) example of an unexpected request from the British civil authorities was the Royal Navy being asked to help deal with the flow of refugees, including many unaccompanied children, trying to cross the Channel—one of the world's busiest waterways—from France to seek asylum in unseaworthy inflatables provided by rapacious criminal gangs.[17] The task of protecting fishing grounds after Brexit may be another issue where greater defense support is sought for surveillance and, where necessary, intervention. Taking COVID-19 as an example, current British doctrine distinguishes between;

- MACC, local military aid to civil communities in trouble, such as local service units helping with distribution of essential medical supplies to care homes in the current COVID-19 crisis, at the initiative of local commanders to respond to requests using existing readily available resources.
- MACM, aid to civil ministries, nationally organized and approved by central government as well as the Defense Secretary, such as running COVID-19 testing clinics and helping build emergency hospitals, on repayment from central contingency funds.
- MACP, armed military assistance to the civil power, including defense budget-funded explosive ordnance disposal and Special Forces capabilities on standby. Thankfully, COVID-19 is well short of generating civil unrest but planners need to consider extreme circumstances where the impact of a future catastrophic natural disaster might be sufficient to cause social dislocation beyond the capacity of the police to control.

The opportunity of the current national security strategic review being conducted by the British government[18] should be taken to examine whether the missions envisaged by the current UK categories of military support to the civil authorities, and how they are funded, manned, and equipped, match the needs of tomorrow. I hasten to add here that doing more to prepare for major hazards must not replace the requirement for the possession of military power capable of deterring threats, or when necessary, allowing lethal force to be used effectively in combat. But it may mean some redefinition of the purpose of defense forces in protecting the state.

It is also important to recognize that the "total defense" of the citizen provided by the Protecting State cannot be delivered by defense departments and the armed forces alone. As with COVID-19, the brunt of the effort will rest on civil resources, not least public health and enforcement of regulations. The primary role of the civil authorities in planning for military support needs to be protected to avoid any perception of a gradual "securitization" of civic life to which the public might be resistant. That is a route we have seen some countries in the global south go down, ending with military suppression of democratic politics. And when defense resources are legitimately engaged, those involved must remain conscious of civilian sensitivities, not least in response to the natural instinct to exercise leadership on the part of military officers highly trained to assess and act decisively in difficult situations.

The constitutional situation in the United States is of course different from that in the UK. The UK has no equivalent of the U.S. National Guard available to be called upon by state governors to maintain law and order where some major disruptive challenge results in social breakdown (as happened in parts of New Orleans after Hurricane Katrina), nor the Posse Comitatus Act prohibiting the use of Federal armed forces for law enforcement. But I merely observe that viruses like malware respect no borders, domestic or international—and infectious diseases can be spread maliciously as well as by nature. Ways must be found

Oregon National Guard sets up Oregon Medical Station (Oregon National Guard, March 19, 2020)

to arrive at satisfactory contingency plans within national constitutional settlements.

A common lesson from the COVID-19 experience is the importance of clarity in the doctrine of crisis management that is to be followed for civil emergencies. We all know how to manage external national security threats. Defense doctrine, for example, emphasizes the need for clarity in strategic direction at the top, coupled with delegation or devolution of the authority to commanders and supporting commanders, under defined rules of engagement necessary to enable flexible theater decisions to match actual events on the ground. The worse the crisis, the more authority needs to be pushed down the line since only those in direct contact with the adversary, be that a far-away hacker or an ever-present virus, can know enough to make the optimum decision for that theater of operations or locality. The same principle must apply to the management of major disruptions caused by civil hazards. The doctrine to be followed must be regularly exercised in a variety of different scenarios so that planners have the evidence on which to build contingency plans. During a major dislocation is not a good time to have to construct new command and control doctrine between central and devolved or local authorities and impose it on organizations and institutions for whom it is novel.

Modern communications may give the illusion that those in the center will be able to control a disruptive situation and execute complex operations, but we must expect the fog of war to be always present. In the end, all crises are local in their impact. We all know that the first reports from the scene are always wrong in significant respects. There is a trust issue here too: public promises built on early data conveyed to the media too soon can destroy reputations when retractions are forced.

Getting reliable and timely COVID-19 infection data and analyzing it consistently has clearly tested

both the U.S. and UK governments. There is never enough reliable data available early enough in any crisis, of course. Crisis management means weighing up and using what information there is—from overseas as well as domestic sources—to make probabilistic decisions, and being prepared to reassess when fresh information arrives. The certainties of the clinical researcher waiting for years for the definitive result of random double-blind trials is too high a standard for public health in a crisis. And for politicians, changing minds in the light of strong new evidence emerging is a sign of strength not of weakness of will.

COVID-19 and Information Operations

The COVID-19 pandemic has certainly shaken public trust in our national institutions to do the right thing and to explain their actions sufficiently clearly, transparently, and consistently to the public. There are explicable reasons for this: this coronavirus had not been seen before and the science did not provide unambiguous answers about vectors of transmission, China withheld important and relevant information about the first appearance of the coronavirus, subsequent warnings from the World Health Organization were not sharp enough, concerns over the impact on the economy muted the nature of early public warnings, and so on. But the strategic lesson is that, whatever the reasons, the information domain has created significant problems for both the United States and the UK, and many other nations.[19] Such problems will often be experienced in the case of other disruptive hazards and threats alike.

COVID-19 also happened to hit us on the back of a rising domestic and external tide of social media misinformation, half-truths, and information manipulation. The vulnerability of our democracy to digital manipulation has been emphasized by the Director of the U.S. National Counterintelligence and Security Center.[20] His warning was about the risks to the 2020 U.S. presidential election, but the points made also apply to Russian and other foreign media spreading lies about the coronavirus, with suggestions that it originated in a U.S. military biolab in 2015 (or as one report had it, in a U.S. laboratory in Armenia).[21]

The warning also applies to Russian attempts to hack into UK and U.S. research labs to try to steal information about the vaccines being developed[22]—perhaps to be able to justify the claims on Russian media that Russia already has a COVID-19 vaccine. We also have to be concerned about conspiracy theories being spread, such as the false claim that there is a connection between 5G microwave radiation and vulnerability to COVID-19 that has already resulted in over 50 attacks on mobile phone masts in the UK. Anti-vaxxer disinformation has included conspiracy claims on social media that COVID-19 is being exploited as a pretext to introduce compulsory vaccinations. Our interests will be affected by anti-Western coronavirus disinformation in the global South. As of August 2020, Facebook had placed warning labels on around 50 million pieces of COVID-19-related content.[23] Anti-Western coronavirus disinformation is being deliberately targeted at the global South and is dangerous to local populations as well as to our interests. As Josep Borrell, the High Representative and Vice President of the European Commission, warned in June 2020:

> *Disinformation in times of the coronavirus can kill. We have a duty to protect our citizens by making them aware of false information, and to expose the actors responsible for engaging in such practices. In today's technology-driven world, where warriors wield keyboards rather than swords and targeted influence operations and disinformation campaigns are a recognized weapon of state and non-state actors, the European Union is increasing its activities and capacities in this fight.*[24]

The experience of COVID-19 heightens the urgency of developing an effective deterrent and dissuasion strategy against hostile information warfare. The influence of social media in spreading COVID-related disinformation shows how important it will be for the management of any future disruptive challenge to have secured the cooperation of the big tech and social media companies. And to have thought strategically about how best to lay the foundations for a more discriminating and informed public, for example by making critical thinking and staying safe online, compulsory subjects in our schools.

Sharing Experience in the Application of Analytical Thought

Our intelligence folks know well how to analyze complex data to support timely national decision-making and to exploit data in tactical battlefield situations. In the UK, there is a direct link between the Joint Intelligence Committee (JIC), the heads of the intelligence agencies, and the Prime Minister and senior Cabinet colleagues. The chair of the JIC and heads of the intelligence agencies attend the UK National Security Council. The experience of analyzing and using all-source threat assessments should be drawn on for all forms of disruptive challenges too.[25] Civil analysts and policymakers can use what I call the "SEES" model of analysis; Situational Awareness, Explanation, Estimation and Modelling (the final S standing for Strategic Notice) to enable preemptive measures to be taken to cope with the level of risk we feel we can tolerate, such as investing in resilience.

Situational awareness is trying to answer the questions, "what, when, where, and who," essential today in judging how to respond to the spread of COVID-19, for example by imposing local lockdowns. Getting reliable, timely, and consistent COVID-19 infection data has clearly been a problem for governments. In crisis, there need to be urgent consultations with decisionmakers at all levels of government and the private sector about what data will be central to their assessments, and when it will be needed. An information requirements grid, with any necessary data definitions agreed to, in order to ensure comparability and timescales for reporting, can then be imposed nationally. That allows a battle rhythm to be established for meetings of the National Security Council or other senior decision fora.

Today, meeting crisis information requirements may involve access to sensitive citizen personal data in bulk. There are lessons here from the controversy over the use of mobile phones as COVID-19 alerting instruments. We cannot take for granted that there will be sufficient public acceptance of digital surveillance and of the use of machine learning in artificial intelligence (AI) algorithms, even for national security purposes. A lesson of COVID-19 for the future is the need to develop ethical codes for AI applications in which lawmakers, the tech companies, and the public have confidence.

Apple and Google have released a Bluetooth app that can be used to warn citizens when near a recorded COVID-19 sufferer, which is potentially useful. Virginia is the first state to have adopted it. But the companies refuse for their own data protection reasons to disclose the location of such close encounters with COVID-19 sufferers, preventing public health authorities from establishing heat maps of COVID-19 hotspots.[26] That, I suggest, is a data privacy decision that in a public emergency, is for the democratic state to take, not private companies, no matter how big or important they may be. The UK had to try to develop its own mobile phone app given the restrictions imposed by the companies, with significant delay in the introduction of the system. We cannot permit such situations to arise in the future.

Explanation is the second component needed for satisfactory analysis of a disruptive challenge, answering policymakers' question, "why are we seeing this data?" This involves Bayesian causal inference to test competing hypotheses of why we

observe the data points we do. For example, infection rates that have shown the greater vulnerability of some minority communities to COVID-19 might have a number of contributory explanations, such as statistically significant environmental conditions of greater overcrowding and multigenerational housing occupation, greater presence in occupations requiring direct contact with the public such as public transport, or factors associated with incidence of diabetes, or other reasons. Policy responses will depend on the choice of explanation. The task is to choose the explanation that best fits the available facts (and with the least evidence against it). As we acquire more evidence-based explanations of the behavior of the COVID-19 virus, we can be more confident in moving to the third step in analysis, estimation and modelling.

Estimates of how situations may evolve can be produced for decisionmakers, provided that there is a sufficiently robust explanatory model of the situation being faced, thus enabling questions to be answered about "what next or where next?" Modelling will try to answer questions about, "what will happen with this or that intervention" and show events unfolding in different ways, of course, dependent on the assumptions and key parameters the analyst chooses. We have seen this with many differing estimates of the COVID-19 spread, such as the impact of differing assumptions about the persistence of antibodies in those who have been infected and the impact of lockdown and sanitary measures in the average rate of infection (the R number).

The general lesson is the need for an open dialogue among the expert communities advising on the results of their modelling and the policymakers seeking the right combination of responses. The latter must always remember that the answers they get from the professionals will depend upon the exact questions they ask, and the professionals must be clear about why they are being asked those questions. It is also a truism of intelligence work that the absence of evidence is not evidence of absence. A professional judgment that there is currently little or no risk of some outcome X will correctly reflect evidence that the precursors of X have not been observed. But such a statement must not be interpreted as meaning that the professionals see no *future* risk of X. The answer you get depends upon the question you ask.

It is important that the analysts are trained not only to give government their "most probable" estimate but also highlight less likely scenarios where the consequences would be severe if they were to happen. It was the worst case estimate of deaths due to COVID-19 that finally jolted British ministers out of their complacency and into ordering a national lockdown on March 23, 2020. The Prime Minister tested positive for the virus a few days later.

Obtaining *strategic notice* of possible *future* challenges is a fourth important step in the SEES model and one that involves different modes of thinking, about whether to identify black swans or grey rhinos.

Having strategic notice is to be aware of the possibility of wildcards and long-term developments that may help answer important policy questions of the "how could we best prepare for whatever might hit us next?" type. Disruptions take many forms. Some will relate to scientific or technological breakthroughs (such as quantum computing). Some will come from shifts in global power balances. Some from natural forces, such as the emergence of the COVID-19 virus.

For some sources of disruption, it is possible to establish from past experience how frequently they are likely to arise. In such cases, likelihood can be expressed as a "one in 50 years event" or "1 in 100 years" event. For example, the U.S. Geological Survey (USGS) routinely measures the San Andreas fault near Parkfield in central California, where a moderate-size earthquake has occurred on the average of every 20–22 years for about the last 100 years. Since the last sizeable earthquake occurred in 1966, the

USGS estimates that Parkfield has a high probability for a 5–6 magnitude earthquake before the end of this century.[27] It must be borne in mind that even very unlikely events with non-zero probability can—and do—happen. The 2008 financial crash was just such a "long-tailed" event. For other risks, data is increasingly available to allow trend analysis, from which long-term warnings can be inferred, as in sea level rises due to polar ice sheet melts. For most natural hazards, likelihood estimates allow a form of strategic notice, but tactical warning of such events should not be expected, so there will inevitably be surprise and dislocation when they happen. But given sensible anticipatory investment in mitigation measures, we need not be so surprised by surprise itself.

The methods of horizon-scanning are well-known in seeking strategic notice of approaching dangers. The term derives from the ancient practice of having a sailor in the crows' nest of the ship scanning the horizon for the first signs of the masts of the enemy fleet appearing over the horizon. But strategic notice is a wider concept. If looming danger is identified early enough, it may be possible to preempt it. A historical example will illustrate the point. The Spanish intention to land an army in England in the 1560s was uncovered by secret intelligence, and when reporting indicated that an invasion fleet was being assembled, preemptive action was taken to prevent the force ever leaving harbor, which Francis Drake achieved by raiding the Spanish fleet while still at anchor in Cadiz. One advantage of having adequate strategic notice is that it can cue the search for intelligence for the first signs of the anticipated risk (a lesson from COVID-19 as well).

We cannot know the future and we cannot afford to prepare for everything. Having strategic notice of a range of possible significant threats allows us to weigh precautionary steps, especially those that are likely to be robust against a variety of scenarios, such as stockpiling PPE.

When Preemptive Systems Fail

Those four analytical processes described in the preceding section as the SEES model of rational assessment, are conceptually distinct. When governments fail to get a clear warning or to understand its import, this failure can be due to different problems arising at each stage.

We know there can be analytic failures in situational awareness when the first threatening signs are concealed, overlooked, or misinterpreted. This is inevitable to some extent in a dangerous and chaotic world. It may turn out that there were missed opportunities to warn of the seriousness of COVID-19, especially given that the Chinese authorities have a history of not being open about internal affairs. The global outbreak of COVID-19 was certainly a tactical surprise, but it should not have come as a strategic surprise.

Sometimes there are failures of policy response to some disruptive challenge when the explanatory models being used to understand what is going on miss some key features. This can lead to the desired ends of the policy response and the means of delivering it not being aligned (such as when local lockdowns following spikes in infection fail due to insufficiently rapid results from track and trace). And sometimes when, however logical the resulting policy might appear to be to its drafters, assumptions made in the model estimating the effects of the response turn out to be wrong: for example, assuming that all sections of the public will buy equally into mask wearing. It must be accepted that often new policy approaches will have to be crafted in situations of great uncertainty, as with a novel virus of initially unknown characteristics. Strong leadership is what makes a big difference in order to quickly generate a sense of purpose in circumstances where danger looms and to guide the political class and public to reframe their expectations accordingly.

We should also recognize from the COVID-19 experience that there can be specific "warning failures" that fall into the cracks between adequate

Anti-Mask Protest - Coronavirus (COVID-19) Sheffield, UK (Tim Dennell, July 18, 2020)

foreknowledge and appropriate reaction—hearing but not listening. Warning is a deliberative act. It is being pro-active. Warning is more than writing an intelligence estimate or a scientific paper.

An effective warning is a loud shout to senior leadership (and later to the public) for attention:

- A strong knowledge claim about a potentially worrying development
- An assessment of why it really matters if it happens to us
- Sufficient illustration of how current policies and systems may fail in order to drive home the message that precautionary action is needed now to avoid disaster if the risk materializes. For example, with COVID-19, a mismatch between the assumptions made in extant contingency plans of central government and the practical availability of ventilators or testing facilities on the ground.

Warnings powerfully bring together the intelligence, scientific and—where appropriate—public health assessments with honest and rigorous policy analysis. They are unlikely to be spontaneously effective. Processes are needed within government that allow for professional assessments to be provided, without the risk of politicization, but then brought together with policy analysis to form an effective and robust warning system for senior national security leadership.

National security planning today must encompass the potential impact of major hazards as well as the more traditional malign threats facing the nation. Such a wider view of national security planning, examining all the events that could have a major impact on the safety and security of the citizen, has an important dimension of public psychology. The public must have confidence that the potential risks are being satisfactorily mitigated so that normal life can continue freely

and with confidence. There are existing national security processes that provide the basis for decisions on precautionary measures and investment in resilience through the provision of situational awareness, explanation, estimation, and strategic notice, thus allowing better management of malign threats. A modern approach to national security needs comparable and compatible processes to decide how to mitigate the serious global hazards that may lie ahead for our people and for our shared interests. PRISM

Notes

[1] I am grateful to the DOD Joint Staff SMA Program for the opportunity to discuss these ideas with planners in the Pentagon and the UK MOD at an online seminar on August 13, 2020.

[2] U.S. Commerce Department, July 30, 2020, news release, available at <https://www.bea.gov/news/2020/gross-domestic-product-2nd-quarter-2020-advance-estimate-and-annual-update>.

[3] UK Office for National Statistics, Statistical Bulletin, August 6, 2020, available at <https://www.ons.gov.uk/peoplepopulationandcommunity/healthandsocialcare/conditionsanddiseases/bulletins/coronavirustheukeconomyandsocietyfasterindicators/06august2020.>.

[4] As set out by Douglass Barrie, Nick Childs, and Fenella McGerty, "Defense Spending and Plans: will the pandemic take its toll," *Military Balance*, April 1, 2020, available at <https://www.iiss.org/blogs/military-balance/2020/04/defense-spending-coronavirus>.

[5] UK Government, *National Risk Register*, 2008.

[6] A relevant Interpol warning can be found at <https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats>.

[7] See the analysis of the 2000 fuel crisis, available at <http://www.iwar.org.uk/cip/resources/PSEPC/fuel-price-protests.htm>.

[8] An example of the importance of the time discount rate is shown by the arguments over the pathbreaking Stern Report on the economic impact of climate change. See Kenneth J. Arrow, "Global climate Change: A Challenge to Policy," *The Economists' Voice* 4, no. 3 (2007), available at <https://www.degruyter.com/view/journals/ev/4/3/article-ev.2007.4.3.1270.xml.xml>.

[9] Such as is given in the Intelligence Services Act of 1994 that defines the roles of GCHQ and the Secret Intelligence Service (MI6), and in the Investigatory Powers Act of 2016 that authorizes the use of bulk access methods by the intelligence agencies. See the Intelligence Services Act of 1994, available at <https://www.legislation.gov.uk/ukpga/1994/13/contents>. See also the Investigatory Powers Act of 2016, available at <https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted>.

[10] Royal Navy, "Royal Fleet Auxiliary *Mounts Bay* Scores £40m Drugs Bust," press release, February 7, 2020 (in the Caribbean with a U.S. Coast Guard team).

[11] David Omand, *Securing the State* (London: Hurst, 2010), ch.1.

[12] Peter Hennessy, *The Secret State* (London: Allen Lane, 2002) and David Omand, "The Dilemmas of Using Secret Intelligence for Public Security" in *The New Protective State*, ed. Peter Hennessy (London: Continuum Books, 2007).

[13] On the health security dimension specifically, see Filippa Lentzos, Michael S. Goodman, and James M. Wilson, "Health Security Intelligence: Engaging Across Disciplines and Sectors," *Intelligence and National Security* 35, no.4 (2020), 465–476, and the other articles in that special issue on Health Security Intelligence.

[14] Catherine Philp, "States trying to steal vaccine secrets, security agencies say," *The Times*, May 6, 2020.

[15] A "Grey Rhino" is a highly probable, high-impact yet neglected threat, akin to both the "elephant in the room" and the improbable and unforeseeable "black swan." Gray Rhinos are not random surprises, but occur after a series of warnings and visible evidence.

[16] James Kenneth Wither, "Back to the Future: Nordic Total Defense Concepts," *Journal of Defense Studies* 20, no. 1 (2020).

[17] "Home Office Seeks Help over Migrant Crossings," BBC, August 8, 2020, available at <https://www.bbc.co.uk/news/uk-53704809>.

[18] Ministry of Defense, "Defense Pledges to Evolve Faster on the Years Ahead," press release, July 3, 2020, available at <https://www.gov.uk/government/news/defense-pledges-to-evolve-faster-in-the-years-ahead>.

[19] Lawrence Freedman, "Strategy for a Pandemic: The UK and COVID-19," The Survival editor's blog, June/July 2020, 25–76, available at <https://www.iiss.org/blogs/survival-blog/2020/05/the-uk-and-covid-19>.

[20] "Statement from NCSC Director William Evanina: Election Threat Update for the American Public," Office of the Director of National Intelligence, August 7, 2020, available at <https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public>.

[21] A catalog of false Russian media stories about COVID-19 can bsound at the Disinformation Review website, available at <https://mailchi.mp/euvsdisinfo/dr196-881757?e=2b235c697e>.

[22] Chris Fox and Leo Kelion, "Coronavirus: Russian spies target Covid-19 vaccine research," BBC, July 16, 2020, available at <https://www.bbc.co.uk/news/technology-53429506>.

[23] Kate Jones, *Regulating Big Tech: Lessons from Covid-19*, Chatham House Web site, June 10, 2020, available at <https://www.chathamhouse.org/expert/comment/regulating-big-tech-lessons-covid-19>.

[24] European Commission, "Coronavirus: EU strengthens action to tackle disinformation," press release, June 10, 2020, available at <https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1006≥. See also Jennifer Rankin, "China joins Kremlin on EU's list of active disinformation threats," *The Guardian*, June 11, 2020.

[25] David Omand, *How Spies Think: Ten Lessons from Intelligence* (London: Penguin Viking, 2020).

[26] Jami Mills Vibbert, et al., "Covid-19 Tracing Apps: what privacy law will apply," Arnold and Porter Web site, June 10, 2020, available at <https://www.arnoldporter.com/en/perspectives/publications/2020/06/covid-contact-tracing-apps-what-privacy≥.

[27] U.S. Geological Survey, "The San Andreas Fault," last modified November 20, 2016, available at <https://pubs.usgs.gov/gip/earthq3/safaultgip.html>.