GLOBAL STRATEGY FORUM

EDITION No. 44 - NOVEMBER 2020

*The 44th in our series of expert comment and analysis, by **Lord Stirrup KG GCB AFC**, Marshal of the Royal Air Force; Chief of the Defence Staff (2006-2010); and GSF Advisory Board member. As always, the views expressed are those of the author and not of Global Strategy Forum unless otherwise stated.*

The Security Of Critical National Infrastructure

In January of 2020 the UK Government decided to allow Huawei to participate in the construction of Britain's 5G telecommunication system, provided that the Chinese firm's market share was restricted to 35% and confined to the non-core elements of the network. The announcement of this decision caused uproar both here and in the United States. Opponents pointed to Huawei's connections to the Chinese Government, while defenders averred that the company was politically independent and trustworthy. The US Administration claimed that the involvement of Huawei meant that secret intelligence would be put at risk, and threatened to reconsider the Five Eyes arrangements.

How was one to sort the facts from the hyperbole in these often intemperate exchanges? I heard evidence from one expert who believed we would be mad to involve Huawei in our network; I saw a convincing presentation from another who was certain that the risks could be managed. The concerns about secret intelligence were surely overblown: we take it as a given that any mobile communication network is insecure, whoever owns and operates it, and we certainly do not pass classified information on it. But it was also clear that the arguments about Huawei's independent status did not hold water: in the first place, Chinese law requires companies to co-operate with the government; and in any case, a Chinese company simply does not say no to the Chinese Communist Party.

In the event, the sanctions that the US Government imposed on Huawei caused the UK to think again, and to announce that all of the company's equipment would be removed from our national network by 2027. But while that particular issue was resolved, the arguments it raised left open the question of how well equipped we were as a nation to identify and secure our critical national infrastructure, and how exposed we might be to attack on this front. Technological advances bring with them exciting opportunities to do

new things, or to do old things in new ways, but they also introduce new vulnerabilities. And the more complex and interconnected society becomes, the more vulnerable it is to shocks. The protection of national infrastructure is not a new issue, but it is one of ever increasing urgency.

In considering the matter, the first thing we have to decide is what we mean by the term national infrastructure. The Government defines it as 'those facilities, systems, sites, information, people networks and processes, necessary for a country to function and upon which daily life depends. It also includes some functions, sites and organisations which are not critical to the maintenance of essential services but which need protection due to the potential danger to the public (civil nuclear and chemical sites for example).' This is a very wide ranging definition, and it would probably be easier to list those things which did not come under it (leisure and entertainment facilities, for example) than those which did.

The constituent elements fall within thirteen separate sectors: chemical, civil nuclear, communications, Defence, emergency services, energy, finance, food, government, health, space, transport and water. Given the number of sectors and the breadth of their coverage, it is clear that to talk in terms of the blanket protection of national infrastructure is absurd. So how do we place sensible limits on the problem and bring it within the bounds of the manageable?

An important step in that process is to consider not just the criticality of infrastructure to the functioning of the country but also its vulnerability to potential threats. The chances of a physical attack on our roads, bridges and railways, for example, are perhaps less than those of a disruption to the traffic management systems on which they depend. The same is true of many other aspects of our life: it is the connectivity and the command and control systems of our infrastructure that are most vulnerable, which is why cyberattack has been identified as a Tier 1 threat to the United Kingdom.

So far, so much accepted wisdom. But in our justified enthusiasm to acknowledge the importance and challenges of cyber security we should not ignore the potential for devastating physical attacks, particularly from rogue or terrorist groups. The contamination of a city's water supply, for example, would have appalling consequences for its inhabitants, and for the nation more widely. As ever with risks, one has to consider both the likelihood and the consequences in order to assign a priority, and thus to focus our efforts and resources most efficiently. This is, of course being done, but there is one great weakness in the methodology: our judgements may turn out to be wrong. Indeed, given that error is fundamental to the human condition, we should take it for granted that we will be wrong to some degree or other. I shall return to this point later, but first I want to address another definitional problem – that of security.

What do we mean by the security of national infrastructure? We do not, in my view, mean invulnerability. We should certainly seek to defend critical areas from attack, but a defender always has certain disadvantages. The choice of when, where and how to attack lies with the assailant, and the defender is, at least at first, outside the observe, orient, decide and

act loop. This problem is particularly acute when the space or activities to be defended are widely spread. We cannot therefore work on the assumption that an attack will fail, no matter how well we prepare; quite the opposite, in fact: we have to assume at least a degree of success. So the security of our national infrastructure becomes a question not of how to prevent attacks entirely, but of how well we can absorb and recover from them.

In its first report in May of this year the National Infrastructure Commission acknowledged as much, and recommended an architecture which was able to anticipate challenges, to resist, absorb and recover from attacks, and to adapt accordingly. They called on the Government to set resilience standards, to appoint regulators to oversee regular stress testing, and to require infrastructure operators to produce long term resilience standards. Some actions have already been taken. The Natural Hazards Team within the Cabinet Office has established a Critical Infrastructure Resilience Programme, and they are working with Government Departments to develop Sector Resilience Plans, but these do not directly address the issue of deliberate attacks on our infrastructure.

All of this seems to me to throw up two different categories of question. What policies and actions would best protect our infrastructure from attack and achieve the necessary resilience; and how do we provide the necessarily rapid assessments and directions to counter the effects of such attacks?

On the first point, the Huawei example would seem to suggest restricting the provision of parts of our infrastructure to trusted suppliers and operators. But who are they, and how are they to be engaged? They cannot be drawn solely from the ranks of 'British' companies (whatever that means in today's globalised business environment), since we do not have the mass, the spread or the technologies within our economy to meet all of our own needs. It is certainly possible to identify less risky 5G suppliers than Huawei, but not ones who are risk free. Even where we do have a national capability to provide and operate parts of our infrastructure, problems remain. Is the Government to identify such 'national champions' in selected areas of business?

This may be necessary in some very restricted areas, but such dirigisme has a poor track record in the UK, for two principal reasons. First, the Government is not very good at identifying winners. Secondly, in order to remain in business such champions need a regular drumbeat of UK orders, which in turn stifles competition and efficiency. There are many salutary examples of this in the history of Defence Procurement. A more productive approach might be to decrease reliance on one or even a few suppliers, and thus to build a degree of redundancy into the most critical parts of our infrastructure. This would not be the cheapest solution, at least in the short term, but the level of insurance that it provides might be well worth paying for. The Government needs to develop an approach that balances cost, risks and resilience, and that constantly monitors and rebalances this equation in the context of our complex and dynamic world.

This requirement, alongside my earlier propositions on the inevitability of wrong judgements and the expectation that some

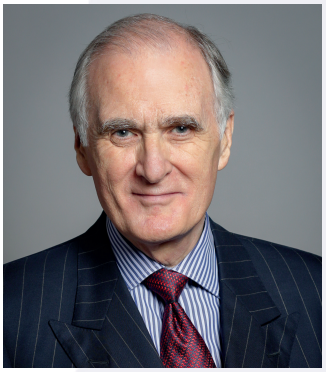
attacks will succeed, at least in part, brings me to my final point. Things move fast in the world of technology, and they will move even faster during a determined attack on our infrastructure. If we are to respond successfully, if we are to absorb the first blow, recover from it and reshape ourselves for the future, we will need two things: agility and adaptability. Agility in this sense is our ability to respond quickly to those things we did not or could not foresee; to change our systems, plans, and indeed our thinking on the fly; to check and then outmanoeuvre our opponents. Our resilience and ability to recover will depend on this. Adaptability, on the other hand, is about our ability to change our longer-term posture in the light of emerging threats and opportunities, and to learn from both failure and success. Agility keeps us in the fight and helps us to master immediate challenges; adaptability maintains our readiness in a changing world.

Neither of these crucial attributes can be delivered by the Government, or by a Government Committee. Those bodies can and should formulate policies and allocate resources, and we have made some progress in this regard, but we also need a much more flexible arrangement to provide effective command and control of both our detailed preparations for and our response to attacks on our infrastructure. The Government has partly acknowledged the problem with the establishment of the National Cyber Security Centre, but this does not address the issue of critical national infrastructure more widely. I believe that we need to establish the core of an organisation that can develop doctrine and procedures, that can carry out stress tests and exercises, that can form a basis of practical experience to inform Government policy on infrastructure, and that can direct the assessments of and responses to attacks. It need not be a large body, but it should be readily and easily expandable in times of tension or crisis, and it should regularly exercise its various functions. Its relationship to the National Cyber Security Centre is an open question; should the former be expanded to incorporate the wider infrastructure issues, or should there be a more federated solution?

There are of course a number of other actors and agents to be factored into the equation, many of them in the civil sector – indeed, their existence is one of the reasons why we need a structure that will provide unity of command. A COBRA committee does not meet this requirement; it can and should give policy direction, but it is not able to run operations. We need a properly established and flexible authority if we are to provide the agility and adaptability essential to the maintenance of the facilities and systems upon which our national life depends.

Lord Stirrup
November 2020

Marshal of the Royal Air Force
The Lord Stirrup KG GCB AFC



House of Lords official portrait