Originally published on 'Europe's World' October 1 2013, Autumn 2013

The more advanced an economy is, the more vulnerable it becomes to cyber-attacks. David Omand, who as a top UK civil servant dealt with cyber security policy, looks at the resilience EU countries need to build into their infrastructure protection plans

-

By **David Omand**

Visiting Professor at King's College London and a former UK Security and Intelligence Co-ordinator and Permanent Secretary of the UK Home Office

Commentary by **Bruce Schneier**

Writes about security, technology and people. Author of Liars and Outliers: Enabling the Trust That Society Needs to Thrive

Twenty years ago this article would have highlighted the 'ring of steel' put around the critical infrastructure of the City of London to keep out the Provisional IRA's bombers. Ten years ago, it would have focused on the measures taken to prevent a 9/11-style attack on European capitals by Al-Qaeda. Today, the major challenge to infrastructure, security and economic well-being comes from the threat of cyber-attack.

It is a hot topic. Last year we saw a cyber-attack on Saudi Aramco, which supplies around a tenth of the world's oil; that destroyed or compromised around 30,000 computers and 2,000 servers. In that same month, cyber-attackers crippled Qatar's RasGas natural-gas company email and other administrative systems. Both attacks are believed to have been by Iran, although it is notoriously difficult to provide courtroom evidence as to where an attack originates – although inferences can be drawn from secret intelligence.

The ability to conduct cyber-sabotage against critical infrastructure exists, and will increase, and both the U.S. and Europe are playing catch up. The Washington Post earlier this year leaked the top secret U.S. Presidential Policy Directive 20, which calls on America's national security leaders to develop destructive cyber-warfare capabilities that "can offer unique and unconventional opportunities to advance U.S. national objectives around the world, with potential effects ranging from the subtle to the severely damaging." The UK (and no doubt other

major European powers) is now investing resources in understanding these technologies.

We must not expect that in the future restrictive policies or sanctions can be imposed on a country – even with the weight behind them of the UN Security Council – and not expect cyber retaliation. We are currently witnessing hostile cyber reconnaissance of key critical infrastructure in the U.S. and Europe. So far these have just been exploring and probing for weaknesses, but I can confidently predict that the ability to sabotage infrastructure will improve. There is an active black market in techniques and knowledge of vulnerabilities, and proliferation of these represents a major risk for Europe.

"We must not expect that in the future restrictive policies or sanctions can be imposed on a country – even with the weight behind them of the UN Security Council – and not expect cyber retaliation"

For much of resilience planning, of course, the difference between malign threat and natural hazard is less important than mitigating the impact on society. How long until services can be restored is the principal pre-occupation. Unexpected disruptions of normal life are still more likely to come from accidents or natural hazards and disasters like earthquakes and floods than from deliberate sabotage. The most demanding scenarios are those where related risks are likely to cascade in a domino effect presenting problems that link quite different sectors. This may occur with advanced cyber-attacks; the interaction of European energy distribution and telecommunications systems being a case in point, and electricity supply and water treatment would be another. The cyber vulnerabilities of critical infrastructure are relatively uncharted territory for Europe.

The more advanced a region is in terms of its dependence on digital technologies, of course, the more vulnerable it is to cyber-attack. That is proving true right across Europe as cyber infrastructure increasingly spans borders. And our economic future in Europe depends on managing these risks down to the point where confidence is maintained. European cyberspace has to be seen as a safe enough place not just to do business, but also for the use of cyber technology to innovate and create wealth. The nightmare scenario is that cyber-crime, espionage, subversion and sabotage could cause such a loss of the confidence that the markets and indeed the general public would doubt whether they can operate safely and securely in Europe's cyberspace.

So what can be done? The UK uses security planning to assess likely losses as the product of a number of factors. First, there's the number, skill level and degree of motivation of the groups who might wish to launch an attack. Then, there is the vulnerability to attack of society, together with its networks, systems and infrastructure. Third, there's the scale of the initial impact – whether it be social, financial or reputational – when an attacker gets through our defences. Finally, there's the duration and therefore the cost of the ensuing disruption before normal services can be resumed.

These factors can be multiplied together to give the expected value of the total loss to be faced. The good news is that all four of these factors can be significantly influenced if governments and the private sector act together.

In reverse order, we can address them as follows. We can reduce the time taken to get back to normal by ensuring there is a core of capabilities in the critical information and communications infrastructure to provide the IT capability to help repair and reinstate damage in other critical infrastructure sectors such as finance.

Who is going to pay for this capability? Most of Europe's infrastructure is in the hands of the private sector, although usually in industries that are in part regulated by the state. It should therefore be a licence condition for any company operating critical systems that they must maintain such core capabilities. Regulators already have to ensure their industry complies with national, European and international safety legislation, and now we have to add cyber security to that. In that way we can ensure a level competitive playing field, and in most cases we must accept that the costs will in any case have to be passed on to the consumer.

Moving on to the next factor, we can reduce the scale of initial impact by building real time situational awareness of attacks that is shared between governments and the private sector. Government has to show it can be trusted by industry with this sensitive information. Any information about attacks and anticipated attacks has to be shared at network speed between the machines patrolling our cyber frontier, government intelligence agencies, law enforcement, the impacted private parties and other actors who need to be forewarned before they suffer the same attack.

"Regulators already have to ensure their industry complies with national, European and international safety legislation, and now we have to add cyber security to that"

The largest short-term impact on the risk can come from the third factor in the risk equation, reducing vulnerability. That means much more cyber security education and acceptance by business and industry of the importance of protecting information networks. Boardrooms need to recognise the commercial risks they run if they don't invest in security, including the handling of employees to minimise insider risks. And they need to ask who are the technical experts who have access to the heart of the infrastructure (the Edward Snowdens) and whether or not just one person should have the keys to the kingdom.

The biggest test of the UK's approach to reducing vulnerability came with the Olympics last year. In the 18 months before the Olympics, I chaired nine table-top exercises in the UK government's COBR situation centre, with the senior players who would be in charge on the day. The aim was to think through scenarios involving different kinds of risk to public safety, including a cyber-attack on the infrastructure. Full-scale live exercises then tested the readiness of all involved, including the games managers from the London organising committee and their volunteers, the police, local authorities, transport operators, key operators of the critical infrastructure, central government, border and immigration authorities, the Foreign Office along with the armed forces, intelligence agencies and other cyber response mechanisms. The Olympic Games passed without major incidents, cyber or otherwise, and such attempts as were made to disrupt the games and defraud the public were foiled. It is nevertheless highly likely that over the next five years one or more EU countries will face some sort of advanced cyber threats.

Finally, the likelihood of attack can be reduced by catching and prosecuting lower level hacktivists and criminals, and making their activities harder. Countering really advanced attacks, however, will depend on a combination of intelligence-led active defences that are ready to respond proportionately to an attack (but not necessarily symmetrically and not necessarily in cyberspace) coupled with the threat of using all elements of national power should there be a devastating attack. We also need to see the development of accepted international norms of behaviour, and a setting of limits for misbehaviour.

A small start has been made on this with the agreement in the UN Group of Governmental Experts on Cyber Issues that international law, especially the UN charter, applies to cyberspace. The internationally accepted laws of armed conflict, for example, aim to minimise civilian suffering when conflict occurs, and that principle applies to attacks on civilian infrastructure in the cyber realm. These are steps that need active European support. There has also been an agreement between Washington and Moscow to reduce the risk of conflict in cyberspace through real-time communications about cyber incidents of national security concern, and that approach could be extended.

For the future, we need agreed norms that reflect the fact that all advanced trading nations stand to lose from the instabilities that cyber-attacks can generate, especially those that result from nations fearing that in a major international crisis their critical military, space and national financial and other infrastructure has been compromised. All the major trading nations stand to lose from the economic damage a loss of confidence in cyberspace would lead to, not least those in Europe.

Commentary by **Bruce Schneier**

Writes about security, technology and people. Author of Liars and Outliers: Enabling the Trust That Society Needs to Thrive

Understanding the threats in cyberspace

The primary difficulty of cyber security isn't technology – it's policy. The Internet mirrors real-world society, which makes security policy online as complicated as it is in the real world. Protecting critical infrastructure against cyber-attack is just one of cyberspace's many security challenges, so it's important to understand them all before any one of them can be solved.

The list of bad actors in cyberspace is long, and spans a wide range of motives and capabilities. At the extreme end there's cyber war: destructive actions by governments during a war. When government policymakers like David Omand think of cyber-attacks, that's what comes to mind. Cyber war is conducted by capable and well-funded groups and involves military operations against both military and civilian targets. Along much the same lines are non-nation state actors who conduct terrorist operations. Although less capable and well-funded, they are often talked about in the same breath as true cyber war.

Much more common are the domestic and international criminals who run the gamut from lone individuals to organised crime. They can be very capable and well-funded and will continue to

inflict significant economic damage.

Threats from peacetime governments have been seen increasingly in the news. The U.S. worries about Chinese espionage against Western targets, and we're also seeing U.S. surveillance of pretty much everyone in the world, including Americans inside the U.S. The National Security Agency (NSA) is probably the most capable and well-funded espionage organisation in the world, and we're still learning about the full extent of its sometimes illegal operations.

Hacktivists are a different threat. Their actions range from internet-age acts of civil disobedience to the inflicting of actual damage. This is hard to generalise about because the individuals and groups in this category vary so much in skill, funding and motivation. Hackers falling under the "anonymous" aegis – it really isn't correct to call them a group – come under this category, as does Wikileaks. Most of these attackers are outside the organisation, although whistleblowing – the civil disobedience of the information age – generally involves insiders like Edward Snowden.

This list of potential network attackers isn't exhaustive. Depending on who you are and what your organisation does, you might be also concerned with espionage cyber-attacks by the media, rival corporations or even the corporations we entrust with our data.

The issue here, and why it affects policy, is that protecting against these various threats can lead to contradictory requirements. In the U.S., the NSA's post-9/11 mission to protect the country from terrorists has transformed it into a domestic surveillance organisation. The NSA's need to protect its own information systems from outside attack opened it up to attacks from within. Do the corporate security products we buy to protect ourselves against cybercrime contain backdoors that allow for government spying? European countries may condemn the U.S. for spying on its own citizens, but do they do the same thing?

All these questions are especially difficult because military and security organisations along with corporations tend to hype particular threats. For example, cyber war and cyberterrorism are greatly overblown as threats – because they result in massive government programmes with huge budgets and power – while cybercrime is largely downplayed.

We need greater transparency, oversight and accountability on both the government and corporate sides before we can move forward. With the secrecy that surrounds cyber-attack and cyberdefence it's hard to be optimistic.