EUROPE NEEDS A "SOCIAL CONTRACT" TO COMBAT CYBER ATTACKS

SUMMARY

All of us in Europe face a non-stop cyber-assault that is unprecedented in its magnitude, persistence and the speed with which attack vectors change to respond to defensive strategies. Awareness of the threat has put cyber security at the top of the EU's political and social agenda, with broad agreement that "something must be done".

Unfortunately, the current EU Commission draft NIS Directive relies on an outdated regulatory approach, originally designed to meet the challenges of the 18th century, and then updated in the 19th and 20th century as technologies developed. These models are too slow and cumbersome to manage the digital environment of the 21st century. They will probably not be effective, and they could even undermine our ability to create a sustainable system of cyber defence.

We need new, more flexible and dynamic models to address the enormous unfamiliar challenges that arise from the ubiquitous nature of digital technology and the inherent vulnerabilities that come with it. These challenges are simply too complex for governments to manage alone. We need to develop and exploit a new partnership between governments and the businesses that own and operate the critical infrastructure, that provide the services essential to a modern economy and that hold the personal data of almost all European citizens.

We also need to understand the cyber threat in a broader context. It is not just about technology, but also has significant economic and public policy implications.

The Internet Security Alliance (ISA) and the Cyber Security Council Germany (CSCG) propose a modern "Social Contract" between industry, governments and citizens. This "Social Contract" will leverage market economies to create a

sustainable system of cyber security while incentivizing innovation, investment and economic development.

UNDERSTANDING THE ECONOMICS OF CYBER SECURITY

We must start by correcting a major misconception: that cyber security is primarily a technical issue to be handled merely by mandating compliance with some regulatory measure.

The point is that technological analysis can only describe HOW cyber-attacks occur. If we want a sustainable system of cyber defence, we also need to understand WHY the attacks occur and WHAT the real damage is. Designing technology security policy without considering economics is as misguided as constructing economic policy without considering technology.

Cyber security cannot be considered in a vacuum. Today's digital networks are the backbone and central nervous systems of modern commerce and culture. It is essential to carefully consider the effects that security measures may have on productivity, innovation, job creation and economic development, and to weave this analysis tightly into our "security" policy.

Discussions on the interplay between economics and cyber security have often been characterized by superficial analysis and unsubstantiated assumptions. What we need is a detailed and careful analysis of this interplay in order to develop policies, which will assure Europe's economic future as well as safeguarding our systems, and the personal data they hold.

So WHY are our cyber systems under attack? The answer is straightforward: it is because all the incentives favour the attackers:

- Cyber-attack methods are cheap and easy to access - they can be purchased on the Internet for just a few hundred Euros. And looked at from the "business" perspective of the criminal, even the so-called "Advanced Persistent Threats (APTs) are comparatively cheap. This is particularly true when digitalization allows the same attacks to be used repeatedly on thousands of different targets.

- Modern cyber attackers can quickly and cheaply adapt their attack methods in response to the defensive systems they encounter (one of the main reasons why imposing a static regulatory regime is completely ineffective).

- Meanwhile, cyber-crime is enormously profitable - so profitable that it is now the crime of choice for organized criminal syndicates, even out-stripping the international drug trade.

On the other hand, the economics of digital defence are much less attractive:

- Defenders are almost inevitably a generation behind the attackers. As a result, they must deploy new unanticipated and often expensive defences at short notice. This compromises strategic planning because it is extremely hard to demonstrate Return on Investment (ROI) on issues that have been prevented.

- Law enforcement has had virtually no impact on the problem. Less than 1% of cyber attackers are successfully prosecuted.

Although private sector investment in cyber security has more than doubled in the past 5 years ---now approaching $100 billion annually (1)---multiple large-scale empirical global studies show that the single biggest obstacle to deploying effective security is cost. (2)

Further complicating the economic balance between cyber-attack and defence is the fact that private entities must now defend themselves from attack from nation states or nation state affiliated proxies. No private entity can reasonably be expected to match the resources of a major nation state, its military or its sponsored proxies. Yet state-sponsored attacks have already been documented and may well be growing.

GOVERNMENTS AND BUSINESS ASSESS THE THREAT RATHER DIFFERENTLY

The prevalence of nation-state cyber-attacks raises another critical but under-appreciated fact: governments and industry understand and address cyber risk in different ways, each perfectly legitimate from their own different perspectives.

There is no such thing as "absolute security". Private enterprise is interested in maintaining what it sees as a commercially acceptable level of security, measured almost completely in economic terms. So for example, companies may accept a certain level of "leakage" (e.g. from pilfering), because their cost benefit analysis shows that the financial loss from security breaches is less than the cost of increasing security to prevent them.

This commercial risk-based level of security may often fall below what a government - with its broader responsibility to protect the state and its citizens – will find acceptable. Governments must consider not just economic but also non-economic requirements (e.g. national security), and these may require a higher level of security than businesses need using their commercial criteria.

Therefore, while private enterprise and governments use the same networks, they may quite legitimately have different views of what counts as "adequate" security. Finding a way to bridge the gap between commercial and government security is a unique cyber security problem.

CYBER-SECURITY AND BUSINESS EFFICIENCY

One of the most important and least understood aspects of the cyber security equation is the growing trade-off between business competitiveness and digital security.

It has often been suggested that business efficiency and productivity would generate adequate security investments to resolve cyber security issues without government intervention.

Unfortunately, the reverse is true: the deployment of modern digital technologies and business practices that are essential to economic competitiveness actually drive industry to be increasingly less secure. Cyber security is not just a technical issue, but it includes many other factors, including processes, education and awareness, threat management and the implementation of guidelines. All these aspects have to be coordinated in a holistic security concept. In addition, this security concept has to be well aligned with the threat and potential damage level, as well as with the necessary investment in people, organisations and technical issues. In the end there has to be a return on investment.

The last decade has seen a vast global array of technological innovations for businesses. These are often necessary for businesses to remain competitive, yet they undermine digital security. To list just a few examples:

- Supply Chain Security. Virtually all manufacturing is now done through the use of long international supply chains. While these supply chains create enormous cost effectiveness they are virtually impossible to fully secure.

- BYOD (Bring Your Own Device). The near ubiquitous diffusion of smart phones and tablets has created a generation of people who come to work expecting to use their own devices to conduct company business. Permitting such behaviour is often an important factor in attracting top-

flight younger employees, it can create substantial business savings, and yet the security issues are obviously multiplied tremendously.

- Cloud Computing. A recent international survey found that 68% of information security professional studies had "little or no faith" in the security of information in the cloud, including 48% who had already put their data in the cloud. Why would nearly half of security people put their data in a location where they had no faith in its security? Because of the enormous ---virtually irresistible---economic benefits of deploying this less, secure technology.

Of course, businesses do take steps to mitigate the risks of these and other insecure practices. However, virtually all these steps will inflict financial costs on a business. The bottom-line is that economics must be an intrinsic part of any public policy for cyber security.

WHY TRADITIONAL REGULATION IS NOT THE ANSWER

In the traditional regulatory model, a government agency determines requirements, which are then mandated upon citizens and businesses. This model largely originated in the 18th century with modifications in the 19th and 20th centuries. While the process of improvement was fairly slow and static, it was appropriate for the times and technologies it was addressing.

The digital world in general is different, and the cyber security landscape is particularly different. Digital technology tends not to fit well into traditional regulated categories, which makes compliance and enforcement difficult:

- The technology changes almost constantly and is deployed very differently by users with major differences apparent even within single corporate structures.

- Attack methods vary widely and change almost constantly, so that it is difficult to keep the regulations responsive to current threats.

- Compliance with outdated or ineffective regulations can be costly and time-consuming, without adding significantly to actual security. In fact, it may divert scarce security resources away from emerging threats.

- The attribution of cyber-attacks is extremely difficult and assigning liability is unreliable. Cyber systems and digital traffic, not to mention attack methods, easily traverse traditional national boundaries and it can be difficult to establish jurisdiction. Indeed, an overly broad assertion of jurisdiction can drive commerce toward more accommodating domains and cause economic disruption.

- While some elements of regulation, especially in industries where the economics of the industry inherently involves regulation maybe integrated into a modern approach to cyber security, the traditional model alone cannot be relied on to provide an effective or sustainable system of cyber security. There can be an added value through not standardizing certain economies of scale, as it would make successful attacks against whole industries much harder to carry out.

THE DRAFT EU NETWORK INFORMATION SECURITY (NIS) DIRECTIVE

How does current EU policy on cyber security policy line up with these arguments?

Unfortunately, in its draft NIS Directive, the EU Commission seems to follow the outdated notion that cyber security is primarily a technical issue. Moreover, it seems to have little appreciation of the complicated economics that underline the cyber environment. In fact, the EU policy proposals would apply a largely

inappropriate traditional regulatory structure, which is likely to be ineffective in managing the quickly evolving and dynamic threat we face from cyber-attacks.

To take some specific examples, the draft NIS Directive requires that:

- Member States (MS) should impose requirements that 'guarantee a level of security appropriate to the risk presented'. However, it is left unclear how much security is 'sufficient', or what level of investment and organizational effort would a business would need to undertake to 'guarantee' its security. The fact is that enforcement measures taken after an event and against an ill-defined scale will only create confusion and uncertainty. This in turn will compromise investment, both in security and in the competitive business processes required to achieve other high priority EU goals such as sustained economic growth.

- Market operators and public administrations should provide mandatory notification of any incidents that have a 'significant impact' on its core services. But it provides no further guidance on what sort of incidents trigger mandatory notification – a sure recipe for uncertainty in practice.

- Stakeholders should report to a 'national competent authority' (NCA) responsible for enforcing the Directive, rather than the voluntary or informal reporting in other countries. A concern here is that many critical infrastructure sectors already have reporting infrastructures. The administrative burden associated with additional and duplicated reporting obligations could take away from scarce compliance resources.

- MS should undertake a significantly enhanced oversight role in the investigation of non-compliant entities, security audits and the issue of binding instructions to market operators.

- MS should adopt “effective, proportionate and dissuasive” sanctions for non-compliance. Exactly what this means and how such sanctions will be reconciled between MS are unclear.

Compounding the uncertainty is a simultaneous reform of EU Data Protection laws, which began in January 2012 and is expected to be voted on by Parliament before the EU elections in May 2014. While the draft NIS Directive and Data Protection reform are separate initiatives, there will be a significant overlap between security and breach notifications. This is because a data breach could also be a security incident, while not all security incidents will involve data breaches. The overlap will inevitably lead to confusion, and will inevitably subject the private sector to even more conflicting demands and costs.

In addition to the uncertainty, steaming from the aforementioned simultaneous reforms comes the lack of communication and coordination among the member states. This further increases uncertainty and creates unnecessary red tape because of the already existing regulations concerning security and breach notifications on the national level. Regulations, which companies doing business in those nations, have to follow. Furthermore, some member states do not even have a national cyber security strategy, which should be the starting point for improving the cyber security situation.

In summary, with the EU regulatory approach, industry will have to disclose security breaches to regulators without control over that information will have to submit to compulsory regulatory audits and will be sanctioned for failure to comply.

AN ALTERNATIVE – A 'SOCIAL CONTRACT' MODEL

The Internet Security Alliance and the Cyber Security Council Germany proposes that the EU Commission should consider an alternative model, based on a social contract, a partnership between industry, government and science. In this approach, government provides economic incentives for private companies to go beyond what they regard as a commercially appropriate level of security, thus providing enhanced security for both governments and individuals.

This operating model recognizes that the private sector possesses resources and expertise for cyber-security, which outstrip those available to governments. It aims to incentivize private companies to constant innovation in security standards, practices and technologies, including techniques that may well be uneconomic to deploy on a strictly commercial basis.

Government's role would be to promote the voluntary adoption of such standards, practices and technologies by making market incentives available to "good actors", those private companies that voluntarily agree to upgrade their cyber security posture beyond the "commercially necessary" level. ,

Governments can also assist by modelling preferred security behaviour such as by implementing sound security practices and increasing investment in critical infrastructures they own and operate. For example, in the newly elected government in Germany has committed to spend at least 10% of their IT budget on security. By benchmarking proper security behaviour, and working with the academic community to develop metrics for evaluating the cost effectiveness of these approaches in relation to the quantified damages of cyber attacks, government can improve private sector security without causing market distortions. Governments can also enhance security by reforming their own procurement practices to promote increased cyber security, help to develop the

private insurance market and reward good actors with regulatory forbearance and streamlined processes.

.

The United States government is already moving down this path. In 2012, it abandoned its centralized government regulatory approach, one very similar to that now under discussion in the EU presently. Instead, it has opted for an enhanced version of the partnership model.

In the US model, the President requested a government agency (NIST) to work with industry through a structured programme to develop a "framework" of cyber security standards and practices. Once this framework is complete (by 14 February 2014), the US government will encourage private entities to adopt it on a voluntary basis underpinned by a set of market incentives. Four different government agencies (DHS, Commerce, Treasury and DOD/GSA) have the task of developing incentives that may be applicable to various critical industry sectors, on the understanding that no single incentive will meet all private sector needs.

The emergence of the US model in parallel with discussions in Europe on the EU NIS Directive is significant for several reasons:

- EU companies will increasingly be placed at a competitive disadvantage *vis-à-vis* their US counterparts. Not only will the Americans not share the financial costs of regulation being placed on EU firms, but they will also be receiving market incentives not available to EU companies.

- With increased economic motives to practice good security behaviours, American companies are liable to become increasingly secure in comparison to their EU counterparts making them more attractive business partners and magnets for outside investment.

- All international companies will be required in practice to accommodate both the US and EU systems. This will increase costs and divert resources that would be better devoted to innovation and job creation - without actually enhancing cyber security.