

**THE HOUSE OF LORDS
SELECT COMMITTEE ON THE EUROPEAN UNION
Sub-Committee F (Home Affairs)**

**INQUIRY INTO
EU POLICY ON PROTECTING EUROPE FROM LARGE SCALE CYBER-ATTACKS**

Memorandum by Dr Stefan Fafinski

Introduction

1. I am pleased to accept the invitation of the Committee to give evidence in response to its inquiry into EU policy on protecting Europe from large-scale cyber attacks. This evidence is restricted to my personal areas of expertise and is submitted on an individual basis.¹ For the avoidance of doubt, the views expressed in this memorandum are my own and must not be attributed to any organisation.

2. This memorandum covers the section of the Inquiry concerning International responses. It is structured with a discussion of the area followed by responses to some of the individual questions raised by the Committee. A much fuller exposition of my views is available in my book *Computer Misuse: Response, Regulation and the Law*,² an electronic copy of which I have supplied to the Clerk with kind permission of Brian Willan of Willan Publishing, on the understanding that the electronic copy of the book will not be made public.

¹ I am a Director of Invenio Research Limited. I have over twenty years experience in the information technology industry, holding senior management positions in software product design, development and programme management. I have subsequently researched, published and lectured extensively on e-crime, computer law and computer misuse and won the 2006 British Association for the Advancement of Science Joseph Lister Award for my work on cybercrime. I am a Chartered Engineer, a Chartered Scientist and a Chartered Information Technology Professional. I am a Court Liveryman of the Information Technologists' Company, the City of London Livery Company for Information Technology. I am also a Fellow of the Institute of Directors, the British Computer Society and the Royal Society for the Encouragement of Arts, Manufactures & Commerce. I am a Member of the Society for Computers and Law, the British Society of Criminology, the Society of Legal Scholars, the Socio-Legal Studies Association and the Fraud Advisory Panel. I hold a Bachelor of Laws degree with first-class honours and a Masters degree in Natural Sciences from St John's College, University of Cambridge. My doctorate from the University of Leeds concerned the legal and extra-legal governance of risks arising from the misuse of information technology.

² Fafinski, S, *Computer Misuse: Response, Regulation and the Law* (Willan Publishing, Cullompton, 2009).

International responses

3. The Commission's desire for a governance network that crosses the public-private divide is not surprising. In 1994, the Bangemann Report considered that the exploitation of the new technologies required to participate in 'the new industrial revolution' would require 'partnership between individuals, employers, unions and governments dedicated to managing change'.³ This partnership would mean 'developing a common regulatory approach'⁴ and thus reflected the European policy objectives of flexibility, legal certainty, harmonisation and technological neutrality.
4. The Commission produced a report in 2001 entitled 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime'.⁵ This report echoed the economic risks associated with computer misuse that were raised in the debates leading to the enactment of the Computer Misuse Act 1990 some ten years previously.
5. The Commission went on explicitly to acknowledge that there are potential extra-legal means of governance which have a role to play alongside legal regulation, proposing a number of non-legislative actions.
6. The first of these was the establishment of an European Union forum to 'enhance co-operation' between law enforcement, internet service providers, network operators, consumer groups and data protection authorities. This forum would aim to raise public awareness of risks, promote best practice, develop counter-crime tools and procedures and encourage the development of early warning and crisis management mechanisms. Such a forum would represent a dynamic networked approach to computer misuse which would be significantly more flexible and responsive than any potential legislative response. The second was the continued promotion of 'security and trust' through products and services with 'appropriate' levels of security and more liberalised use of 'strong' encryption techniques. The third was increased training of law enforcement staff and further research in forensic

³ Bangemann, M and others, 'Europe and the Global Information Society' (the Bangemann Report) (1994) <<http://ec.europa.eu/archives/ISPO/infosoc/backg/bangeman.html>> accessed 18 November 2009.

⁴ Ibid, 4.

⁵ Commission (EC), 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime' COM (2000) 890, 26 January 2001.

computing. The final area was a study to 'obtain a better picture of the nature and extent of computer-related crime in the Member States'.⁶

7. The 2005 Framework Decision⁷ identified the threats arising from attacks against information systems as 'organised crime' and the 'potential of terrorist attacks against information systems which form part of the critical infrastructure of the Member States'.⁸ The nature of these threats is distinct from the economic concerns raised in the Bangemann Report. However, the Framework Decision does reiterate the desire to approximate the criminal law in an attempt to transcend jurisdictional difficulties between states in the interests of:

...the greatest possible police and judicial co-operation in the area of criminal offences...and to contribute to the fight against organised crime and terrorism.⁹

8. The backdrop against which the Framework Decision is set appears to be emphasising the protection of public interests. This was made explicit in the earlier proposal for the Framework Decision which considered the nature of the primary threat was that to communication network operators, service providers, e-commerce companies, manufacturing industries, service industries, hospitals, public sector organisations and governments themselves.¹⁰ The Council also drew reference again to the 'considerable' economic burden associated with such threats.¹¹
9. Similarly, the European Commission's later Communication 'towards a general policy on the fight against cyber crime'¹² reinforced the need for further training of law-enforcement personnel, further research, the development of technical measures to counter 'traditional' crime (such as fraud) in electronic networks and

⁶ Ibid, 31-2.

⁷ Council Framework Decision (EU) 2005/222/JHA of 24 February 2005 on attacks against information systems [2005] OJ L69/67.

⁸ Ibid, recitals [2].

⁹ Ibid, recitals [8].

¹⁰ Commission (EC), 'Proposal for a Council Framework Decision on attacks against information systems' COM (2002) 173 final, 19 April 2002, 3.

¹¹ Ibid.

¹² Commission (EC), 'Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime' COM (2007) 267 final, 22 May 2007.

private-public co-operation in the exchange of information and the raising of public awareness.

10. The United Nations considered that priority should be given to the provision of technical assistance to Member States, in order to provide a 'level playing field'¹³ and thereby harmonising technical capability rather than legal regulation.
11. The G8 Action Plan¹⁴ recommended that there should be a collaborative effort between state and industry to ensure that new technologies are 'policeable': that is, they facilitate the investigation of computer misuse via the collection and preservation of robust evidence. This introduces technological design as an additional potential tier of governance. Moreover, the G8 stresses the involvement of industry in the development of secure systems and participation and co-operation in civil contingency planning.
12. The OECD produced a set of guidelines for the security of information systems and security.¹⁵ This provided a set of complementary principles for 'participants'. 'Participants' is a broadly-defined term encompassing 'governments, businesses, other organisations and individual users who develop, own, manage, service and use information systems and networks'.¹⁶ The principles to which the participants are expected to adhere are awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management and reassessment. The resulting 'culture of security' is one in which these participants take responsibility for their own safety while remaining flexible and co-operative in prevention, detection and response to incidents and respecting the legitimate interests of others. Risk assessments enable the 'selection of appropriate controls' which underpins security management of systems containing components for which security has been an 'integral part of system design and architecture'. This culture is reflexive, undergoing a constant process of review, reassessment and modification.

¹³ United Nations, "“Around the clock” capability needed to successfully fight cybercrime, workshop told' UN Doc SOC/CP/334 (25 April 2005).

¹⁴ G8, 'Meeting of Justice and Interior Ministers of the Eight: Communiqué' (10 December 1997) <<http://www.usdoj.gov/criminal/cybercrime/g82004/97Communique.pdf>> 3 accessed 18 November 2009.

¹⁵ OECD, 'Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security' (OECD, Paris, 2002)

<<http://www.oecd.org/dataoecd/16/22/15582260.pdf>> accessed 18 November 2009.

¹⁶ Ibid, 7.

13. There is clearly an overlap between many of the areas proposed by the various organisations. These fall into a number of broad categories founded on co-operation, information sharing, reflexivity and responsiveness.

CERTs

14. In general terms, a CERT is an organisation that studies computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security.¹⁷
15. For Van Wyk and Forno, a CERT exists 'to minimise the impact of an incident on a company and allow it to get back to work as quickly as possible'¹⁸ whereas for Killcrece it should act as a 'focal point for preventing, receiving and responding to computer security incidents'.¹⁹ Wiik refers to the 'new emerging survivability paradigm'²⁰ which proposes that no matter how much security is built into a system, it will never be totally secure,²¹ replacing the traditional notion of a fortress providing full protection against malicious attack.²²
16. Over time, however, such CERTs widened the scope of their services from purely reactive emergency response towards the more proactive provision of security services including preventive services such as issuing alerts and advisories and providing training on incident management capability, performance standards, best practices, tools and methods. In the late 1990s the term 'Computer Security

¹⁷ ENISA, 'Inventory of CERT activities in Europe' (September 2007)
<http://enisa.europa.eu/cert_inventory/downloads/Enisa_CERT_inventory.pdf> accessed 18 November 2009.

¹⁸ Van Wyk, KR and Forno, R, *Incident Response* (O'Reilly and Associates, Sebastopol, 2001) 21.

¹⁹ Killcrece, G and others, *State of the Practice of Computer Security Incident Response Teams* (Carnegie Mellon University, Pittsburgh, 2003).

²⁰ Wiik, J, Gonzalez, KK and Kossakowski, K-P, 'Limits to Effectiveness in Computer Security Incident Response Teams' (Twenty-third International Conference of the System Dynamics Society, Boston, 2005).

²¹ Lipson, H and Fisher, DA, 'Survivability – a new technical and business perspective on security' (Proceedings of the 1999 New Security Paradigms Workshop, Association for Computing Machinery, Caledon Hills, 1999).

²² Blakley, R, 'The Emperor's Old Armor' (Proceedings of the 1996 New Security Paradigms Workshop, Association for Computing Machinery, Arrowhead, 1996).

Incident Response Team' (CSIRT) arose to reflect this broadened scope. Both terms (CERT and CSIRT) are synonymous in current usage.

17. There is a growing realisation that some level of proactive service ought to be offered as well.²³ CERTs therefore address different types of risk on a spectrum from serious electronic attacks on the public infrastructure, government departments or the financial services industry, through online fraud and identity theft to less serious (but more prevalent) harms involving general on-line nuisance.
18. The constituency (that is, the set of potential users) of a CERT can include national, governmental or private organisations. Equally, although some CERTs may be ostensibly linked to particular national interests, some are effectively global, such as the NCFTA, whereas others focus on particular industry sectors, such as the Financial Services Information Sharing and Analysis Centre (FSISAC).²⁴
19. Each of these CERTs therefore acts as an independent node, collecting, processing and disseminating information relating to risk, although the differences in their constituencies may mean that the relative prioritisation of risks differs between CERTs. Assuming that each CERT has some data of interest to others, it follows that connecting CERTs which represent both public (state) and private (commercial and individual) interests could produce, in Kjær's terms, a 'network... of trust and reciprocity crossing the state-society divide'²⁵ in the pursuit of shared goals or, in Rhodes' words, an 'interorganisational network... characterised by interdependence, resource-exchange, rules of the game and significant autonomy from the state'.²⁶ In other words, interconnected CERTs could provide a response or readiness network consistent with theoretical conceptualisations of governance.
20. In terms of a networked response to a networked problem, it is necessary to examine the nature and extent of inter-CERT collaboration to establish whether information sharing alone is an adequate response or whether CERTs should build

²³ Killcrece, G and others, *State of the Practice of Computer Security Incident Response Teams* (Carnegie Mellon University, Pittsburgh, 2003).

²⁴ <<http://www.fsisac.com>> accessed 18 November 2009.

²⁵ Kjær, AM, *Governance* (Polity Press, Cambridge, 2004) 4.

²⁶ Rhodes, RAW, *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability* (Open University Press, Buckingham, 1997) 15.

relationships with other bodies and assist with collaborative responses to the problems arising from the cyber-attacks.

Collaboration between CERTs

21. UKCERTs is an informal forum of domestic CSIRTs including government, academic and commercial teams, again designed to encourage co-operation and information sharing between the participants. It also invites UK WARPs to its forum meetings. There are similar forms of national cooperation operating in Austria,²⁷ Germany,²⁸ the Netherlands²⁹ and Poland.³⁰

22. The European Network and Information Security Agency (ENISA) was established in 2004 by Regulation (EC) 460/2004.³¹ ENISA is a European Community Agency; that is a body set up by the EU to carry out a very specific technical, scientific or management task within the Community domain (the First Pillar) of the EU. ENISA's purpose, as defined in its establishing Regulation is that of:

Ensuring a high and effective level of network and information security within the Community and [to] develop a culture of network and information security for the benefit of citizens, consumers, enterprises and public sector organisations of the European Union.³²

23. It does, however, acknowledge that its objectives are without prejudice to non-First Pillar competencies of Member States (such as police and judicial co-operation in criminal matters) and the activities of the States in areas of criminal law.³³ It is specifically charged to 'provide assistance and deliver advice'³⁴ to the Commission and Member States in relation to information security and to use its expertise to 'stimulate broad co-operation between actors from the public and private sectors'.³⁵ Part of ENISA's work is in facilitating co-operation between CERTs. It also supports

²⁷ CIRCA (Computer Incident Response Co-ordination Austria).

²⁸ CERT-Verbund.

²⁹ O-IRT-O.

³⁰ Polish Abuse Forum.

³¹ Council Regulation (EC) 460/2004 of 10 March 2004 establishing the European Network and Information Security Agency [2004] OJ L 77/1.

³² Regulation (EC) 460/2004, art 1(1).

³³ Ibid, art 1(3).

³⁴ Ibid, art 2(2).

³⁵ Ibid, art 2(3).

the member states in setting up their own national or organisational CERTs and provides technical support to close the gaps between the Network Information Security competencies of individual EU Member States. Its 2008 work plan included an initiative to facilitate co-operation between Member States to set up new governmental or national CERTs, acting as a 'good practice knowledge-base and contact broker'.³⁶

24. The European Government CSIRTs (EGC) group is an informal organisation of governmental CSIRTs³⁷ that is 'developing effective co-operation on incident response matters between its members, building upon the similarity in constituencies and problem sets between governmental CSIRTs in Europe'.³⁸ It works to develop measures to deal with large scale network security incidents, facilitating the sharing of information and specialist knowledge and instigating collaborative research in areas of mutual interest specifically related to the operational work of governmental CSIRTs. It differs from ENISA in its more limited membership: ENISA is concerned with facilitating communication between all European CERTs, whereas the EGC focuses only on governmental CSIRTs.
25. The Task Force of Computer Security and Incident Response Teams (TF-CSIRT) exists to promote collaboration between European CSIRTs with a research and education constituency.³⁹ It was established as part of the technical programme within the Trans-European Research and Education Networking Association (TERENA). It has similar aims to the EGC in promoting collaboration, promulgating common standards and procedures for responding to security incidents and providing training for new CSIRT staff.
26. The Trusted Introducer (TI) programme was also established under the auspices of TERENA.⁴⁰ It recognises the nature of the trust relationship which is a necessary condition for collaboration between nodes within a governance network. While the inter-CSIRT trust network was originally based upon personal recommendation between members of the particular CSIRTs involved, as the number of CSIRTs

³⁶ ENISA, 'ENISA Work Programme 2008' 24
<http://www.enisa.europa.eu/doc/pdf/management_board/decisions/enisa_wp_desig_ver_2008.pdf> accessed 18 November 2009.

³⁷ France, Germany, Finland, the Netherlands, Sweden, UK, Norway and Switzerland.

³⁸ <<http://www.egc-group.org>> accessed 18 November 2009.

³⁹ <<http://www.terena.nl/tech/task-forces/tf-csirt/>> accessed 18 November 2009.

⁴⁰ <<http://www.trusted-introducer.nl/>> accessed 18 November 2009.

proliferated and staff moved on, this personal recommendation method became unwieldy at best. TI therefore exists to facilitate trust between European response teams by formally accrediting CSIRTs who wish to join its community. On a similar regional basis, APCERT was established by CSIRTs within the Asia Pacific region, aiming to improve cooperation, response and information sharing among CSIRTs in the region. APCERT consists of 20 CSIRTs from 14 economies.

27. In October 1989, a major incident called the 'WANK'⁴¹ worm'⁴² highlighted the need for better communication and coordination between teams. The Forum of Incident Response and Security Teams (FIRST) was formed in 1990 in response to this problem. Since that time, it has continued to grow and evolve in response to the changing needs of the incident response and security teams and their constituencies. The FIRST membership consists of teams from a wide variety of organisations including educational, commercial, vendor, government and military.
28. Finally, the Central and Eastern European Networking Association (CEENet) comprises 23 national research and education CERTs. It is primarily a knowledge network which shares information regarding computer network security.

Effectiveness of CERTs

29. The effectiveness of CERTs can be considered at two levels. The first of these is the internal effectiveness of the CERT itself; the ability of the CERT to deal with its workload and service its constituents as a reflection of its technical, financial, organisational and management capability. The second is the effectiveness of inter-CERT communication. If the networked response offered by CERTs is to be valuable, it follows that the propagation of pertinent information between CERTs is key to avoid them existing only as silos of information accessible only to the particular constituency of each individual CERT.
30. In terms of internal effectiveness, the main challenges are described by West-Brown:

To ensure successful operation, a CSIRT must have the ability to adapt to changing needs of the environment and exhibit the flexibility to deal with the

⁴¹ Worms Against Nuclear Killers.

⁴² CERT, 'WANK Worm On SPAN Network' Advisory CA-1989-04 (17 October 1989) <<http://www.cert.org/advisories/CA-1989-04.html>> accessed 25 September 2008.

unexpected. In addition, a CSIRT must simultaneously address funding issues and organisational changes that can affect its ability to either adapt to the needs or provide the service itself.⁴³

31. Therefore, internal challenges are two-fold: adroitness (both technological and organisational) and availability of resources. In terms of resources, as Salomon and Elsa comment, information security is often viewed as a drain since it is a support service rather than a core business activity:

Safeguarding the enterprise itself is a fairly unglamorous task, costs money and is difficult to justify to managers unfamiliar with the potential consequences of not having a strong commitment to IT security.⁴⁴

32. Overstretched resources are a common issue within many CSIRTs. As early as 1994, only six years after the establishment of the US CERT at Carnegie Mellon, Smith commented that:

About the only common attributes between existing Incident Response Teams are that they are under-funded, under-staffed and over-worked.⁴⁵

Moreover, according to Lipson:

Although the sophistication of Internet attacks has increased over time, the technical knowledge of the average attacker is declining, in the same manner that the technical knowledge of the average user has declined.⁴⁶

Therefore, more people have the capability to launch attacks and the scope, frequency and volume of attacks (and hence the need for CERT services) is continuously increasing.⁴⁷

⁴³ West-Brown, MJ and others, *Handbook of Computer Security Incident Response Teams* (2nd edn Carnegie Mellon University, Pittsburgh, 2003) 177.

⁴⁴ Salomon, JM and Elsa, P, 'Computer security incident response grows up' (2004) 11 *Computer Fraud & Security* 5.

⁴⁵ Smith, D, 'Forming an Incident Response Team' (Proceedings of the FIRST Annual Conference, University of Queensland, Brisbane, 1994).

⁴⁶ Lipson, H, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues* (Carnegie Mellon University, Pittsburgh, 2002) 9.

⁴⁷ Killcrece, G and others, *State of the Practice of Computer Security Incident Response Teams* (Carnegie Mellon University, Pittsburgh, 2003).

33. A further complication arises in respect of the scope of 'IT security'. It spans a wide range of activity within which security-related tasks may fall to groups which are not immediately concerned with security as a core function, such as architecture, network operations, IT strategy or server support.⁴⁸ Even where adequately funded and resourced, CERTs must be able to respond swiftly to new forms of technological risk. A CERT organisation should be able to adapt to technological advances relatively quickly. However, the speed of response required in order to be effective is increasing. As Salomon and Elsa comment:

The 'flash-to-bang' time between the discovery of new vulnerabilities (or configuration errors) and the exploit thereof on a wide scale has narrowed considerably...Even assuming efficient processes and good communication, the sheer scale of many corporate security organisations makes effective and timely countermeasures difficult.⁴⁹

34. Communication between CERTs also poses a number of potential problems. As EURIM commented,⁵⁰ those running CERTs differ in 'cultural values' and approaches to security. These range from those who only engage with trusted organisations to those which purport to provide open services to all. Moreover, some are more open to communication with peer organisations than others and some exist to protect the commercial interests and intellectual property rights of themselves and their customers. A Police Officer in interview offered an interesting illustration of the importance of the routine administrative matters which underpin CERT-to-CERT communication:

Through our WARP, we got wind of a DDOS attack that was being routed through a country in Eastern Europe. So the obvious thing to do was get in touch with the relevant CERT in that country. Would have been fine – except it turns out that the CERT in question had changed their phone number three years ago and hadn't thought to tell anyone. Certainly would have limited the amount of incoming information they would have got – so,

⁴⁸ Salomon, JM and Elsa, P, 'Computer security incident response grows up' (2004) 11 *Computer Fraud & Security* 5.

⁴⁹ Ibid.

⁵⁰ EURIM, 'Cyber-crime Reporting and Intelligence' (Tackling Crime and Achieving Confidence in the On-line World, Parliament and the Internet Conference, London, 2007).

you see, without some sort of proper day to day coordination and action then all these bodies are next to useless.

35. There are also legal concerns affecting CERTs. Graux comments that CERTs require their own legal expertise in order to develop and apply internal policies as well as to determine whether or not a particular incident requires the involvement of the criminal or civil law. He concludes that the need for international legal cooperation and coordination is paramount, requiring the 'pragmatic availability' of legal channels of communication.⁵¹ There is, therefore, a role for the law to govern and inform the internal framework of the extra-legal response mechanism of the CERT.

WARPs

36. Warning, Advice and Reporting Points (WARPs)⁵² are part of the information sharing strategy of the UK Centre for the Protection of the National Infrastructure (CPNI).⁵³ They are therefore primarily a domestic initiative, covering the public service, local government, business and voluntary sectors⁵⁴ Examples include the National Health Service (Connecting for Health) Information Governance WARP which provides centralised distribution of warnings and advisories, good practice advice brokering and trusted sharing of electronic related security problems and solutions and PENWARP which serves the journalist community.

37. The WARP model is not new or restricted only to the sphere of computer technology. For instance, the Radio Amateurs' Emergency Network (RAYNET)⁵⁵ is a national voluntary communications service for major civil emergencies or related exercises and local community events provided by licensed radio amateurs. It liaises with emergency services, local authorities and other voluntary agencies who could be involved in the integrated management response to major civil emergencies.⁵⁶

⁵¹ Graux, H, 'Promoting good practices in establishing and running CSIRTs – a legal perspective' (ENISA Workshop, 13 – 14 December 2005).

⁵² <<http://www.warp.gov.uk>> accessed 18 November 2009.

⁵³ <<http://www.cpni.gov.uk>> accessed 18 November 2009.

⁵⁴ As at 1 June 2008

<<http://www.warp.gov.uk/Index/WARPRRegister/indexcurrentwarps.htm>> accessed 18 November 2009.

⁵⁵ <<http://www.raynet-uk.net/>> accessed 18 November 2009.

⁵⁶ RAYNET now has an associated WARP (RAYWARP).

The Environment Agency also operates an advisory and response service for flood risk.⁵⁷

38. WARPs are predominantly a 'bottom-up' initiative, although their increasing importance in the area of contingency planning and management of the critical national infrastructure means that they are strategically part of the 'top-down' agenda of the CPNI.
39. Unlike CERTs which generally focus on broader constituencies, a WARP (according to the CPNI) is a 'community based service where members can receive and share up-to-date advice on information security threats, incidents and solutions'.⁵⁸ Therefore, WARPs essentially operate as small-scale CERTs serving a community which may be within a smaller organisation or as a hub to particular organisations or individuals. UKERNA⁵⁹ proposed a model within which WARPs reduce incidents by providing preventative advice and CSIRTs respond to those incidents which do, in fact, occur.⁶⁰
40. There is little regulatory constraint to concern WARPs other than a short Code of Practice which requires little from new WARPs over a willingness to co-operate and share information, maintain effectiveness and not to bring the WARP model into disrepute.⁶¹ Agreement to this Code is a pre-requisite for registration with the CPNI.
41. WARPs, therefore are lightly-regulated 'mini-CERTs' serving similar needs to a more restricted community. As with CERTs, the trust relationship between WARP members is important and one which is stressed by the CPNI as being crucial to their effectiveness. However, given the smaller scale of WARPs as compared to CERTs, it might be expected that there would be considerably more of the former than the latter in operation, although there actually remains a larger number of

⁵⁷ <<http://www.environment-agency.gov.uk/subjects/flood/>> accessed 18 November 2009.

⁵⁸ Ibid.

⁵⁹ Now JANET(UK).

⁶⁰ UKERNA, 'CSIRTs and WARPs: Improving Security Together' (March 2005) <<http://www.warp.gov.uk/Marketing/WARPCSIRT%20handout.pdf>> accessed 18 November 2009.

⁶¹ —, 'WARP Code of Practice v.2.0' (August 2004)

<<http://www.warp.gov.uk/BusinessCase/CodeofPracticeV2.0.pdf>> accessed 18 November 2009.

CERTs than WARPs in the UK at present. Despite this limited adoption, the role of WARPs within the overall framework of governance responses seems theoretically attractive, extending the reach of the extra-legal response network to parties that may not, of themselves, fall within a CERT's constituency or have the capacity or desire to establish a CERT of their own. However, the very existence of WARPs does not seem to be particularly widespread knowledge.

42. For the CPNI, the desire to increase the prevalence of WARPs is clear. It believes that WARPs should become 'endemic' in the future, wherever a need is identified, whilst remaining sustainable, co-operative, flexible and versatile. It further envisages linkage between some WARPs and existing CERTs, with some potentially evolving into full CERTs themselves before concluding that 'the future of WARPs is bright'.⁶²
43. There is limited material available in relation to the overall effectiveness of WARPs. This is probably due to their having been in existence a comparatively short time and being few in number. However, given the similarities between WARPs and CERTs in many respects, it seems reasonable to assume that they may both suffer from similar limitations in terms of capacity and inter-WARP communication. The latter may be less significant, since WARPs are focused on domestic concerns and registered WARPs may use a common communications infrastructure provided by the CPNI.
44. Given the smaller reach of WARPs, they may be considered to be the cyber-equivalent of a Neighbourhood Watch scheme. While there is some element of proactive promotion of WARPs from the CPNI, the protection of individuals from computer misuse is not core to its purpose which is properly concerned with the protection of critical national resources from terrorist or other attacks.

⁶² —, 'The future of WARPs' <<http://www.warp.gov.uk/Index/indexfutureofwarps.htm>> accessed 18 November 2009.

The Commission believes that a pan-European approach is needed to identify and designate European Critical Infrastructures, and that national responses will be fragmented and inefficient. Is this analysis correct? Would multi-national companies be especially in favour of multi-national policies?

45. A pan-European approach would provide greater consistency in determining those infrastructures which are critical to Europe as a whole as well as the individual Member States. National responses may be fragmented and inefficient, but they would allow each Member State to protect those parts of their own infrastructure that may fall outside the pan-European designation. It may be preferable for a pan-European set of infrastructures to be identified, particularly where these span national borders, while allowing Member States to augment these with other infrastructure components as they see fit.

46. It is likely that multi-national companies would welcome multi-national policies which facilitate greater ease of implementation and management.

The Commission draws attention to the emergence of “public-private partnerships” as the reference model for governance issues relating to critical infrastructure protection. However, they see no such partnerships at the European level and wish to encourage them. Are the Commission correct in this aim?

47. Within the various theoretical analyses of risk, there is a common theme of the withdrawal of the direct intervention of the state in the management and regulation of risks in favour of diffuse networks of risk management actors enabling individuals to take responsibility for themselves within the ‘new legal order’ offered through insurance. For O’Malley:

...these responsabilising processes seemingly democratise government through the mobilising of risk and uncertainty. Individuals and communities are made free to choose how they will govern themselves in relation to a host of insecurities.⁶³

48. The question to be considered is how such unforeseen risks should be addressed. This model of risk management by individuals and communities working alongside the state is referred to as ‘governance’.

⁶³ O’Malley, P, *Risk, Uncertainty and Government* (Glasshouse, London, 2004) 11.

49. The ambit of the term has expanded to encapsulate something distinct from government which includes non-state contributors. For example, Hyden considers that:

Governance is the stewardship of formal and informal political rules of the game. Governance refers to those measures that involve setting the rules for the exercise of power and settling conflicts over such rules.⁶⁴

50. For Rhodes 'governance...is about regulating relationships in complex systems'⁶⁵ and for Hirst and Thompson 'governance...is a function that can be performed by a wide variety of public and private, state and non-state, national and international, institutions and practices'.⁶⁶ Inherent in all these definitions is a recognition of something broader than government which includes informal as well as formal rules, described by Kjær as 'networks of trust and reciprocity crossing the state-society divide'.⁶⁷ This notion of some degree of independence from the state is echoed by Rosenau:

Global governance is conceived to include systems of rule at all levels of human activity – from the family to the international organisation – in which the pursuit of goals through the exercise of control has transnational repercussions.⁶⁸

51. As with Hyden, Rosenau's definition of governance also involves the concept of a network: in this instance, a transnational network of states, providing global governance within a framework of international relations. Rhodes provides a complementary perspective:

⁶⁴ Hyden, G, 'Governance and the Reconstruction of Political Order' in Joseph, R (ed), *State, Conflict and Democracy in Africa* (Lynne Rienner, Boulder, 1999).

⁶⁵ Rhodes, RAW, 'The hollowing out of the state: the changing nature of the public service in Britain' (1994) 65 *Political Quarterly* 138, 151.

⁶⁶ Hirst, P and Thompson, G, 'Globalisation and the Future of the Nation State' (1995) 24 *Economy and Society* 408, 422.

⁶⁷ Kjær, AM, *Governance* (Polity Press, Cambridge, 2004) 4.

⁶⁸ Rosenau, JN, 'Governance in the Twenty-First Century' (1995) 1 *Global Governance* 13.

Governance refers to self-organising, interorganisational networks characterised by interdependence, resource-exchange, rules of the game and significant autonomy from the state.⁶⁹

52. As Kjær summarises, definitions of governance focus 'on the role of networks in the pursuit of common goals'. These networks may consist of a variety of state and non-state participants active in a particular area of policy. The degree of cohesion will naturally vary from network to network.

53. Rhodes attempts to draw these definitional strands together in suggesting that the shared characteristics of governance are interdependence between organisations, continuing interaction between network members, game-like interactions rooted in trust and a significant degree of autonomy from the state.⁷⁰

54. It is common ground, then, that governance blurs the distinction between the state and society with the state becoming a collection of networks with no sovereign actor able to steer or regulate. Forms of economic and political organisation are affected.⁷¹ Braithwaite considers that risk management 'decentralises the role of the state' compared with corporations and hybrid public/private regulators.⁷² Offe concurs, stating that:

the outcomes of administrative action are in many areas not the outcomes of authoritative implementation of pre-established rules, but rather the results of a 'co-production' of the administration and its clients.⁷³

55. Lenk considered that the state can no longer control technology by itself and foresaw the potential emergence of a governance approach to its control:

Taken together, badly designed technology, *misused technology* and unmastered technology concur to put society in a position where it can no

⁶⁹ Rhodes, RAW, *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability* (Open University Press, Buckingham, 1997) 15.

⁷⁰ Rhodes, RAW, *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability* (Open University Press, Buckingham, 1997) 53.

⁷¹ Stewart, A, *Theories of Power and Domination: The Politics of Empowerment in Late Modernity* (Sage, London, 2001).

⁷² Braithwaite, J, 'The new regulatory state and the transformation of criminology' (2000) 40 *British Journal of Criminology* 222, 228-9.

⁷³ Offe, C, *Contradictions of the Welfare State* (Hutchinson, London, 1984) 310.

longer aspire to regulating and controlling all details through its political institutions. Well-regulated sectors will co-exist with others from where we may expect influences which trigger the emergence of new types of individual and collective behaviour.⁷⁴

56. This viewpoint acknowledges that the state is not impotent in its ability to regulate networked technologies. Hirst and Thompson comment that ‘if...mechanisms of international governance and re-regulation are to be initiated, then the role of nation states is pivotal’⁷⁵ although the partnership between society and the state has necessarily limited the scope of state intervention.
57. Therefore public-private partnerships are an essential component of the governance approach to managing risk associated with networked technologies and infrastructures. The Commission is correct in its aim that public-private partnerships at the European level should be encouraged.

Are Government operated Computer Emergency Response Teams (CERTs) an appropriate mechanism for dealing with Internet incidents?

58. CERTs have two principal functions. The first is proactively to disseminate information regarding prevention of technical vulnerabilities and threats. The second is reactively to provide assistance in response to particular instances of computer misuse. CERTs exist to serve both public and private interests across a range of constituencies. They may therefore operate from both ‘top-down’ (governmental) and ‘bottom-up’ (private) perspectives. However, in isolation, an inwardly-focused CERT will operate as an information silo; that is, it will not exchange relevant information with other CERTs. Indeed, many CERTs have a closed constituency and may not even desire to participate in such information sharing. This lack of reciprocity is fundamentally at odds with the networked approach required within governance theory, even though the individual CERTs themselves may represent both public and private concerns. Facilitating communication and information-sharing

⁷⁴ Lenk, K, ‘The challenge of cyberspatial forms of human interaction to territorial governance and policing’ in Loader, B (ed), *The Governance of Cyberspace* (Routledge, London, 1997) 134.

⁷⁵ Hirst, P and Thompson, G, ‘Globalisation and the Future of the Nation State’ (1995) 24 *Economy and Society* 408, 430.

between CERTs should therefore lead to a structure more aligned with the governance approach.

59. This has been achieved to a certain extent at both national and international level through various forums of varying degrees of formality, membership and geographic reach. In essence, there is a state-led imperative for co-operation between institutions which often exists only to serve private interests. Provided that there is at least some co-operation, however reluctantly, it follows that CERTs should have a part to play within an overall governance network on the basis that even limited information-sharing is better than none at all.
60. However, in order to achieve a meaningful role within this network, CERTs need to be effective, both internally in their capacity to cope with the nature and extent of their workload as well as externally in the efficiency of their information exchange. Historically, CERTs have been characterised by constrained resources and increasing workload. Moreover, despite the existence of the diverse umbrella co-ordinating bodies, communications between CERTs are inconsistent, depending upon the cultural values and individual priorities of each CERT.
61. Even though an ideal CERT network seems well-suited as a extra-legal response to the problem of cyber-attacks, it must be recognised that CERTs cannot exist in a legal vacuum. The law still has the role of governing and informing the internal framework within which the CERT operates. However, CERTs do offer the advantage of an alternative response beyond that of the law in isolation and bring private concerns and day-to-day technical incidents into the response network.

Will the UK's existing approaches to this policy area be adversely affected by fitting in with a European-wide system – or will this lead to improvements?

62. Provided that the European-wide system allows the UK to deliver at least the same level of protection against cyber-attacks, its existing approach should not be adversely affected by following a pan-European system, and, given the cross-border implications of an attack on many critical infrastructures, should give the UK a greater level of protection from the consequences of the risk of an attack on another Member State.

Is it sensible to develop European-centric approaches at all, or should there be much more emphasis on a worldwide approach? In particular, are US policies consistent with the proposed European approach to the problem?

63. In recognition of the fact that cyber-attacks on the European critical infrastructure could easily emanate from outside the EU it would seem sensible to adopt a worldwide approach. However, the uniform adoption of a global minimum framework within each nation state with clearly defined cross-border co-operation, investigation and assistance provisions is a panacea.

64. This has been most notable in the criticisms levelled at the Council of Europe Convention on Cybercrime.⁷⁶ As Brenner and Clark comment, since it incorporates substantive and procedural law that may not be routine in some Member States then:

...it means implementing the Convention will be a complicated process for many countries, one that will take time. Consequently, even if the Convention proves to be a viable means of improving law enforcement's ability to react to transnational cybercrime, we are unlikely to see any marked improvement in the near future.⁷⁷

65. This view is echoed by Flanagan who further considers delay resulting from the prospect of constitutional difficulties, the propensity of individual legislatures to 'do things their own way' and the 'workings of special interest groups to ensure their input into national implementations all around the world'.⁷⁸

66. Lewis⁷⁹ criticises the effectiveness of the Convention (in common with all international initiatives) on a number of grounds. He considers that there is a lack of incentive for many countries to participate, particularly in those developing countries where computer crime is not yet a significant concern. He further argues that there will be problems with effectiveness even where countries do participate, citing a list of obstacles including the speed at which new technologies are

⁷⁶ Council of Europe Convention on Cybercrime (signed 23 November 2001) ETS 185.

⁷⁷ Brenner, SW and Clarke, LL, 'Distributed Security: Preventing Cybercrime' (2005) 23 *John Marshall Journal of Computer and Information Law* 659, 671.

⁷⁸ Flanagan, A, 'The law and computer crime: Reading the Script of Reform' (2005) 13 *International Journal of Law and Information Technology* 98, 117.

⁷⁹ Lewis, BC, 'Prevention of Computer Crime Amidst International Anarchy' (2004) 41 *American Criminal Law Review* 1353.

developed, differences in certain substantive values between States, different standards for conviction, the imposition of different punishments upon conviction, the failure of many countries to commit adequate resources to fighting computer crime and the lack of any viable international body to coordinate national agencies and enforce international agreement.

67. Weber⁸⁰ also highlights the potential flaws within the Convention, arguing that it will fail without universal participation and will take 'years' to ratify. Lack of worldwide participation could lead to safe havens beyond the Convention's reach, meaning that states will still need to take unilateral action against individuals in countries that fail to join, ratify, implement or enforce the treaty. For Goldsmith, such unilateral assertions of power might encourage accession to the Convention and facilitate global adoption.⁸¹

68. The United Nations has the broadest reach of the intergovernmental bodies covering virtually all recognised states. It has adopted broad resolutions in the areas of computer crime; these are recommendations and compel no action on the part of Member States. Legislative action in the form of a UN Cybercrime Convention to build and improve upon the Council of Europe offering is still considered premature. The UN is instead focussing on providing technical (rather than legal) assistance to Member States thereby harmonising technical capability rather than legal regulation.

69. This approach of providing technical assistance is similar to the that adopted by the UN in relation to terrorism. Following the attacks on the US of 11 September 2001, the UN introduced a two-fold mechanism to facilitate global adoption of effective laws against the financing of terrorist activity.⁸² The problem that the UN faced was that states such as Yemen, for example, were disinclined to take action since such action was inconvenient, not a national priority and difficult to implement for lack of technical expertise. The UN therefore established the Counter Terrorism Committee to which all states were called upon to report on the steps taken to implement its proposals (many of which required legislative action). As well as acting as a focal point for the UN efforts, this Committee also facilitates the provision of

⁸⁰ Weber, AM, 'The Council of Europe's Convention on Cybercrime' (2003) 18 *Berkeley Technology Law Journal* 425, 444-5.

⁸¹ Goldsmith, JL, 'The Internet and the Legitimacy of Remote Cross-Border Searches' (2001) 1 *University of Chicago Legal Forum* 103, 117.

⁸² United Nations Security Council Resolution 1373 (28 September 2001).

'assistance of appropriate expertise'⁸³ to states in furtherance of the objectives set out in the Resolution. Therefore, the UN takes a role of co-ordination and assistance rather than direct coercion. However, this arrangement was only brought into being as a result of the political impetus following 11 September 2001. It is therefore reasonable to assume that that a similar co-ordinated international approach to cyber-attacks would require an event of similar gravity to precipitate it. However, the conceptual idea of co-ordinated international technical assistance remains at least theoretically attractive.

70. In the absence of a concerted and committed global response to the issue, a European-centric policy may be the simplest and most compelling option to protect European interests.

Dr Stefan Fafinski
18 November 2009

stefan.fafinski@invenio-research.co.uk

⁸³ Ibid, art 6.