Ian Brown. *The law and economics of cybersecurity*, eds. Mark F. Grady and Francesco Parisi, *Law Quarterly Review*, 123, 172-175, January 2007.

Grady / Parisi (eds.): The law and economics of cybersecurity. Cambridge University Press (2006)

Using stealth and surprise, the Japanese fleet struck a devastating first blow against the United States Navy in 1941 at Pearl Harbour. Are we facing a similar level of threat to our electronic infrastructures today? Is the Internet the new frontier on which transnational terror networks like al-Qaeda will plan and execute acts of mega-terrorism, as we hear so breathlessly from those selling security (in all of its guises)?

"The Law and Economics of Cybersecurity" is a new collection of essays that approach this subject from a variety of angles. Should government or the private sector take the lead in addressing the threat of cybercrime and cyberterror? What level of transparency is optimal from these actors, both in terms of market efficiency and impact on privacy and other human rights? How far can technological responses obviate the need for regulatory intervention, and what market incentives are required to encourage such innovation?

Editors Mark F. Grady and Francesco Parisi have done a good job in bringing together a wide range of theoretical and political perspectives. At one end of the spectrum we hear a call from Neal Katyal for much stronger criminal sanctions and law enforcement activity based on the "network harm" done to citizens' trust in the Internet, even by trivial hacking attacks. Katyal also argues that social justice demands police intervention as the only alternative to allowing poorer Internet users to fend for themselves in a sea of cyber-predators. Bruce Kobayashi arrives at the same destination via a different route: that private action by associations of organisations will lead to an overspend on public security goods due to the incentives firms have to protect their own networks. At the international level, Joel Trachtman argues that the negative externalities caused by state inaction on cybercrime demands a much stronger, co-ordinated response via international bodies and treaties along the lines of the global measures taken to protect marine security and reduce money laundering and terrorist financing.

Amitai Aviram, Doug Lichtman and Eric Posner instead call for a private-sector led response with limited government intervention. Aviram looks at the regulatory subsidies such as anti-trust exemption given to cybersecurity associations, and argues that such measures must be carefully allocated to prevent the subsidy of inefficient associations and the crowding out of groups with great efficacy. Lichtman and Posner call for stronger statutory or common law indirect liability to be attached to Internet Service Providers, who they claim to be in a unique position to reduce cybercrime by their users as "gatekeepers" to the Internet. Less prescriptively, Peter Swire analyses the conditions under which it will be optimal for companies to share information about security vulnerabilities, and for government agencies to share personal data concerning suspected criminals.

At the far end of the scale comes Randal Picker, who argues against even the use of government procurement power to encourage "biodiversity" in the operating systems and server applications that run the Internet. Picker claims that software "monocultures" are less harmful than has been claimed, and that the early release of buggy software followed by *in situ* patching is an effective approach to promoting software adaptability. Doubtless these conclusions were a pleasant surprise to one of the sponsors of his work, Microsoft Corporation.

The chapter that really stands out is "Peer Production of Survivable Critical Infrastructures" by Yochai Benkler. The author posits that the availability of stored data, processing power and communications bandwidth should be society's key concern, rather than attempts to fortify specific machines and links on the network. Benkler lucidly describes how new technologies such as ad hoc wireless mesh networks, peer-to-peer file systems and distributed computing protocols can ensure this availability in a highly reliable manner. He also shows how economic theories of shareable goods can be used to incentivise the production of these distributed and replicated systems; and suggests policy changes that will enhance their utility to society.

Benkler's careful linking of law, economics and computer science emphasises that the study of cybersecurity must be a highly interdisciplinary effort if it is to capture the nuances from each of these fields. A deep understanding is required of technology's possibilities, and of mechanisms that can regulate and incentivise the development and use of technology that will maximise social welfare. Peter Swire's analysis of information sharing, for example, would be improved with the incorporation of Ross Anderson's results from reliability growth models applied to security vulnerabilities. Few computer scientists would be as uncritically accepting as Randal Picker of Microsoft security strategist Scott Charney's claim that "thousands" of operating systems would be needed to ensure true diversity (or that most recent IT innovation is a happy result of the Windows monoculture.) They certainly would though agree with Picker's contention that much greater use should be made of autarky, or the physical isolation of networks linking critical systems such as those controlling power grids.

The almost complete absence of human rights considerations from the book is disappointing. A criticism of the development of national and international cybersecurity law is that it has been led by law enforcement and interior ministry officials with little input from the members of the judiciary and civil society concerned with freedom in the information age. The Council of Europe's Cybercrime Treaty, touched on by Joel Trachtman, was negotiated in secret and only at the 19th draft (of 27) was comment sought outside the law enforcement community. The UK's Internet surveillance regime is opaque, with little real oversight or consideration of the million-plus UK citizens subject to some form of electronic surveillance each year. The European Union's own Data Protection Supervisor has criticised the recent Data Retention Directive as disproportionate and illegal; whilst the UK House of Lords' EU select committee has recently attacked the Home Office for pushing aside privacy concerns to negotiate an information-sharing agreement with five other large EU members.

Yet several authors of this book make suggestions that would radically increase control and surveillance of Internet users. Lichtman and Posner suggest the introduction of indirect liability for Internet Service Providers, despite the great difficulty ISPs would face in identifying cyber-criminals amongst their customers. Trachtman suggests that ISPs might be "deputised" to patrol their networks, detecting "suspicious" activity and maintaining records of such customers' communications for several years. In a brief aside, he hints that every Internet user might be required to present biometric credentials before gaining access to the network. He also suggests that the threat of cyberterrorism may exceed that of marine-borne terrorism, only one page after pointing out the dangers of the transport of nuclear, biological and chemical weapons by ship!

This is a toxic combination of a lack of perspective on the level of threat, the invasiveness of the policies suggested to meet it, and the real technical difficulties in implementing such policies. Are we facing an "electronic Pearl harbour," or more frequently the equivalent of graffiti sprayed onto a store front? How exactly would ISPs pick through the megabits of data streaming every second to and from each of their broadband users to pick out criminal actions? If that data stream is encrypted, there is little that the ISP can do; and attempts to push ISPs into the role of gatekeepers would act as a strong incentive for the authors of viruses, Trojan horses and Denial of Service zombies to use encryption.

A combination of increased costs and higher liability would also cause ISPs to stop serving their more marginal users. Randal Picker states that certain consumers "shouldn't be using computers or be on the network," but Prof. Lilian Edwards of Southampton University has suggested that any liability regime that has this effect will act as an iniquitous sanction on age, ignorance and technophobia.

"The Law and Economics of Cybersecurity" is a substantial and thought-provoking read that will be useful to academics and policymakers attempting to reduce the harm caused by an undoubtedly growing threat to developed societies. It should though be read with a critical eye, and with a realistic conception of the reality of the potential harm in the medium term. As Harvard's David Isenberg wrote in a Cato Institute commentary: "Does that mean that there is no threat to U.S. computer networks? No. But, to paraphrase the immortal words of Pogo, it means that we have met the enemy, and he is us – that is, our own lackadaisical computing habits, misleading press reporting and government overreaction. Those problems may be worse than the threat itself."