CPGE 2023-2024

oral sessions with C. Hamard

# A large-scale cyber-attack highlights the structural dilemma of the NSA

# *The Economist*, 2017

# IN BRITAIN, doctors could neither access their patients’ files nor make appointments to see those patients. In Russia, hundreds of the interior ministry’s workers sat idle. In China, students were locked out of their theses. As the latest cyber-attack rippled around the globe, infecting at least 45,000 computers in 74 countries, according to Kaspersky Labs, a Russian cyber-security firm, it seemed for a moment that the world was facing digital apocalypse. In the event, catastrophe was averted when somebody found a kill switch, which stopped the malicious software involved spreading further. Untold hours will have to be spent cleaning up the mess. What is more galling than that is that all of this was entirely avoidable.

# From the victims’ perspective, the Great Cyber Attack of May 12th was a typical, if widespread, example of extortion by “ransomware”, to which users of Microsoft’s Windows operating system are particularly vulnerable. After they had received what is known as a “phishing” e-mail, which dupes recipients into installing an infected file, their computer displayed a message which began, “Ooops, your files have been encrypted!” It then went on to tell them that if they wanted to use these files again, they needed to pay a ransom of $300—or, rather, its equivalent in bitcoin, an anonymous cryptocurrency.

# What was not typical was the scale of the attack. This was because the malware involved (named, variously, Wannacry, Wanna or Wcry) is also a type of program called a “worm”. Worms are particularly insidious because, once one has infected a computer, it can use local networks to spread from that machine to others without requiring anybody else to open e-mails or click on links. Wannacry does this by exploiting a vulnerability in some older versions of Windows. Although this weakness was known about, and Microsoft had already issued a software patch to fix it, that patch had not, apparently, been installed as widely as it should have been. In Britain, the National Health Service was badly hit because its IT systems are chronically underfunded. Many hospitals seem to have been using a version of Windows that is no longer supported by Microsoft, making them wide-open to attack.

# A deeper problem is America’s National Security Agency (NSA), which had known about the vulnerability in Windows which Wannacry exploits, and had even built a tool called “Eternal Blue” to exploit that same weakness. “Eternal Blue” was leaked in April by a group of hackers, along with many other such hacking weapons, and was then used by other hackers to turn Wannacry into a fast-spreading worm.

# This points to a structural weakness that will be harder to stop than Wannacry. It is that the NSA is torn between two missions. One is to defend computer systems. The other to attack them, in order to gather information or even to shut them down. The agency thus has an interest in keeping at least some of the vulnerabilities it comes across a secret, so that it can use them for its own purposes (although in this case it had warned Microsoft after the hackers’ leak). (514 words)