

ORAL CONCOURS 2015

ANGLAIS - LVI

Hacking for Humanity

CAMBRIDGE – “Life,” Oscar Wilde famously said, “imitates Art far more than Art imitates Life.” In the case of Sony Pictures’ movie *The Interview*, the world found itself confronted with a further iteration: life imitating art imitating life. The movie’s release sparked international intrigue, drama, and shadowy geopolitical power struggles. It even prompted a grave US Presidential address – all for a simple case of hacking.

Hacking into information systems is nothing new; it goes hand in hand with the emergence of telecommunications. One of the first attacks struck Guglielmo Marconi’s demonstration of radio transmission in 1903, when he communicated from Cornwall to London, 300 miles away. Nevil Maskelyne, a music-hall magician and would-be wireless tycoon, who had been frustrated by the Italian inventor’s patents, managed to take control of the system and broadcast obscene messages to the Royal Institution’s scandalized audience.

Though hacking is as old as wireless itself, much has changed since Marconi’s time. Information networks now blanket our planet, collecting and transferring immense amounts of data in real time. They enable many familiar activities: instantaneous communications, social media, financial transactions, and logistics management. Most important, information is no longer sequestered in a virtual realm, but permeates the environment in which we live. The physical, biological, and digital worlds have begun to converge – giving rise to what scientists refer to as “cyber-physical systems.”

Automobiles, for example, have evolved from straightforward mechanical systems into veritable computers on wheels. The same thing is happening to other consumer goods: We now have connected washing machines and learning thermostats, not to mention Bluetooth toothbrushes and computerized infant scales.

Indeed, cyber-physical systems range from the macro level (think urban transport, like Uber) to the micro (say, the beating of a human heart). [...]

All of this promises to revolutionize many aspects of human life – mobility, energy management, health care, and much more – and may point toward a greener and more efficient future. But cyber-physical systems also heighten our vulnerabilities to malicious hacking, an issue that is being discussed at the World Economic Forum in Davos. Far from being isolated in cyberspace, attacks can now have devastating consequences in the physical world. It is an annoyance when a software virus crashes our computers; but what if the virus crashes our cars?

Malicious hackers are difficult to combat with traditional government and industry tools [...]. Hacking can be carried out anywhere and everywhere, potentially involving multiple networks in obscure locations. It defies conventional retaliation and protection strategies. As then-US Defense Secretary Leon Panetta warned in 2012, given its current systems, the United States is vulnerable to a “cyber Pearl Harbor” that could derail trains, poison water supplies, and cripple power grids.

So, how can such a scenario be prevented?

One option, surprisingly, could be to promote widespread adoption of hacking itself. Familiarity with hackers’ tools and methods provides a powerful advantage in diagnosing the strength of existing systems, and even in designing tighter security from the bottom up – a practice known as “white hat” hacking. Ethical infiltration enables a security team to render digital networks more resistant to attack by identifying the flaws. This may become routine practice – a kind of cyber fire drill – for governments and businesses, even as academic and industry research focuses in the coming years on the development of further technical safeguards.

In general, today’s defenses take the form of autonomous, constantly vigilant digital “supervisors” – computers and code that control other computers and code. Similar to traditional military command-and-control protocols, they gain power in numbers and can quickly react to a broad array of attacks. Such a digital ecosystem strengthens checks and balances, reducing the possibility of failure and mitigating the effects of an incursion.

In such a future scenario, a Hollywood blockbuster might be about networks of computers fighting each other, while humans stand by. It would portray the broader idea of “singularity,” a hypothetical turning point when the artificial surpasses the human. Fortunately, in this case, life is still far from imitating art.