



Sostituzione Mutuo Bersani

Abbassa le rate del tuo mutuo. Fai un preventivo e risparmi !



MONDAY, JANUARY 26, 2015

Empty input field

Empty input field

INNOVATION & TECHNOLOGY

Columnists

Sections

Syndication

Focal Points

About Us

CARLO RATTI [Follow @senseablecity](#)

Carlo Ratti, a member of the World Economic Forum's Global Agenda Council on Future Cities and the curator of the Future Food District pavilion at the 2015 World Expo in Milan, directs the Senseable City Laboratory at the Massachusetts Institute of Technology. [READ MORE](#)



MATTHEW CLAUDEL

Matthew Claudel is a research fellow at the Senseable City Laboratory. [READ MORE](#)

JAN 23, 2015

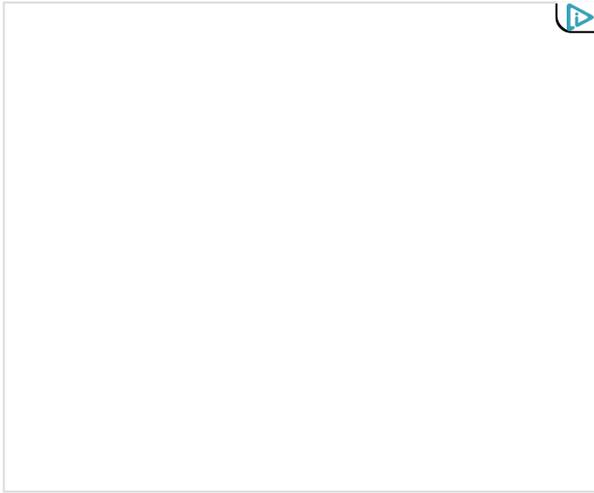
English

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.



ADVERTISEMENT

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). Our very bodies, strapped with connected wearables, are today imbued with more computing power than all of NASA at the time of the Apollo missions.

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 – the Sony Pictures case being a telling example. 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.

[CONTACT US TO SECURE RIGHTS](#)

[POST COMMENT](#)

[READ COMMENTS \(1\)](#)

Read more from *Davos 2015*



As the World Economic Forum convenes in Davos, much attention will be devoted to the usual suspects: Russia, China, the Middle East, and the eurozone. But other global risks – including protracted war, epidemics, inequality, and environmental disasters – have also come into view.

[PREVIOUS](#)

[NEXT](#)

[Have We Become Too Flexible?](#)

[A New Century's New Technologies](#)

COMMENTS

READ COMMENTS (1)

Please sign in or register to leave a comment.

SIGN IN

REGISTER

FEATURED



BUSINESS & FINANCE JAN 17, 2015

Making Sense of the Swiss Shock

MARKUS BRUNNERMEIER & HAROLD JAMES apply some historical lessons to Switzerland's abrupt decision to abandon the franc's euro peg.



ECONOMICS JAN 15, 2015

What Good Are Economists?

ROBERT J. SHILLER argues that public anger at the economics profession is unjustified and unfair.



WORLD AFFAIRS JAN 15, 2015

The War with Radical Islam

JEFFREY D. SACHS on why the attacks in Paris and elsewhere should not be blamed on insanity or evil.

Project Syndicate provides readers with original, engaging, and thought-provoking commentaries by global leaders and thinkers. By offering incisive perspectives from those who are shaping the world's economics, politics, science, and culture, *Project Syndicate* has created an unrivaled global venue for informed public debate.

Columnists**Sections**[Economics](#)[World Affairs](#)[Sustainability & Environment](#)[Business & Finance](#)[Politics](#)[Global Health & Development](#)[Innovation & Technology](#)[Culture & Society](#)[Education](#)**Focal Points****Archive****Blogs****Syndication****About Project Syndicate**[Editorial Board](#)[Project Syndicate, Prague](#)[Submission Guidelines](#)[Contact Us](#)[Jobs](#)