Towards the End of Secrecy: Technological and Human Considerations

Louis Massey
Royal Military College
Kingston, Canada

1. Is 'Openness' possible?

I used to be a technology specialist for the military intelligence community. In addition to developing and maintaining information systems, one of my responsibilities was to keep information secret. When I started in the 1980's, things were easier: information resided on isolated mainframes and if someone wanted to get it out, they had to print it and transfer it to microfilm or attempt to walk out with a stack of classified papers. A few military policemen conducting sporadic searches of staff entering and leaving the facilities was an effective deterrent, at least for the obvious cases. Later, personal computers with floppy disks, or more recently with connectors for small memory sticks, made it easy to copy large amount of information and leave secure areas undetected despite searches that just cannot always be intrusive enough.

And hence the work of Bradley Manning, Julian Assange and Edward Snowden has been made possible. We are well beyond a few pieces of papers or microfilms left for foreign agents in a park drop or a brown envelop with a few pages sent to the New York Times. These modern day dissidents who defy the authority of powerful governments have revealed massive quantity of information which has been circulated world-wide thanks to the Internet and other media.

During my tenure with military intelligence, the last situation I wanted to face was hackers attacking the systems under my responsibility, or accidental or intentional release of classified information by employees. I have to admit: I am culturally biased *towards* secrecy. Although the idea of openness appears to me as a noble one, I must ask: is it realistic in a world dominated by a culture of secrecy?

Secrecy seems to be an essential component of security and national defence. States (and corporations) play a game of hide and seek – hiding as much information from their adversaries (and allies!) while trying to obtain as much information from and about them. Gathering intelligence is of extreme importance to know in advance what others are up to, while keeping information confidential is complementarily just as imperative.

We accept these behaviours as axioms of international relations because it is the way it has always been, and because everybody else is "doing it." Are those valid justifications? Maybe not, but how can secrecy and intelligence gathering be stopped or controlled with the aim of achieving more openness when their very nature makes them almost immune to verification?

“Knowledge is power” may be a cliché, but it is one that is firmly entrenched in our ways.

2. Information Technology: Enabler and Duality

The immense amount of information society generates daily is a powerful incentive to continue inventing faster and more effective Information Technologies (IT) to facilitate information processing, organization and distribution. At the same time, IT also invite more information generation, creating an endless cycle of innovation.

IT is essential in government and international affairs to obtain and manage the large quantities of information to run a country and know what other States are up to. At the same time, from a secrecy preservation perspective, IT is problematic: the ease of copying electronic data on small devices and open access to mass media like the Internet, make obtaining and publishing secret information a much simpler task than it used to be.

There is a continuing debate about the nature of technologies – are they inherently good or bad, or is it how we use them? Are they the prime cause of social change? (see for example: Smith and Marx, 1994; Postman, 1993; Winston, 1998; Harris and Sarewitz, 2012; Feenberg, 2004; Kranzberg, 1986.) To illustrate this debate, one can look at intelligence gathering technologies supporting military operations and State strategic decision-making. Material intercepted on the world telecommunications infrastructure is collected in vast databases and analysed by supercomputers for patterns that may indicate threats. Using mathematical techniques and shear computing powers, encrypted information may be deciphered, resulting in gained tactical or strategic advantage or aversion of a crisis. So-called intelligent “big-data” analytics software sifts through vast amount of linguistic and social relationship information to determine who exchanges information with whom, on what topic, and whether this collates with other information of interest.

These technologies were developed to support the State’s objectives and needs; the technologies did not cause the objectives or the needs. The intentions are noble: to protect peace and freedom; to maintain a stable and secure society in which citizens can enjoy a happy life. At the same time, people within the State apparatus often have the desire to grow their power. This can easily lead to abuses, given that the technological tools are readily available to capture information about honest citizens’ political opinions and private activities.

The recent leaks reported extensively in the media illustrate the wide-range of information gathering activities pursued by governments. It would appear that IT technologies are imbued with agency – given their immense possibilities, they seem to invite abuse.

Drawing from Orlikowski (1992), it can be argued that the polarity in the debate about the nature and determinism of technologies is futile. Technologies, and in our particular case IT, are double-edged swords: they exist in an inextricable *duality*. On one hand, they support states and corporations in preserving and improving their dominant position and ability to exploit and manipulate. On the other hand, IT also allow for more information to circulate more freely, making citizens more aware of issues, facilitating coordination and organization of political and social activism, and overall improving the democratic process.

The same technologies are being used for breaching freedoms and waging wars, but also for solving conflicts, improving human condition and making institutions more transparent (for e.g., Best et al., 2011). It is not about one or the other possible use and causality, but rather about both as intrinsic co-existing realities. As such, technologies are a reflection of our nature as much as our nature is a reflection of our technologies. Historical and cultural realities, opportunities and necessities make us invent technologies, while technologies also affect our culture, our perceptions and the course of History (McLuhan and Lapham, 1994).

IT, at the image of their underlying quantum electronic nature, exist as a duality manifested as improved openness, human rights, and freedom but also as increased potential for abuse, manipulation and control by organizations that master the technological and information landscape.

There is an opportunity for human intervention to keep the balance between the two aspects of IT favourable to 'ordinary citizens;' to favour the good side of IT. How can this be achieved? Transparency by providing open access to all information, particularly information that can be a threat to world security as advocated by Bohr, is a noble enterprise because with a permanent spotlight, better behaviours are often achieved, possibly leading to improved peace, security and overall well-being for humanity. But as I mentioned previously, because of the existing culture of secrecy in state and commercial affairs, and because of the very nature of secrecy openness will probably continue to be an objective difficult to reach for the near future. Although openness may not be implementable as an enforceable and verifiable international 'Rule of Law,' it may nevertheless happen involuntarily and partially thanks to hackers and whistle-blowers, enabled by IT.

3. The Social Role of Hackers

If a state or corporation controls content or information flow, citizens are disempowered. Fortunately, by their fluid nature, IT are difficult to control. It is where the hacker and the whistleblower have an important social role to play by freeing information that would otherwise be kept secret. Their actions help bring the balance of information-power to the citizen side.

Given that IT is widely available and networks rarely perfectly secure, even the most classified information is not immune to unwanted access. As periodically reported in the media over the last few decades, even a teenager with relatively modest means but a high level of creativity can hack into secure systems. Is the threat of involuntary disclosure helping to keep the balance of information power favourable for citizens, thus making it a necessary force in our democratic societies? Drawing from Steven Levy's book *Hackers: Heroes of the Computer Revolution*, one may be tempted to see hackers as heroes rather than criminals. Shouldn't all information be free, meaning open, accessible by all?

In that respect, the hacker (either using advanced technological means or simply walking out of NSA with a memory stick or DVD) plays a key role in social change by causing destabilization. By making public what is secret, insight on hidden processes and information is gained, making the citizen more aware of what is going on and thus enabling calls for changes, better oversight of powerful secretive agencies and in the end overall improved democracy. This form of *involuntary transparency* certainly destabilizes institutions momentarily, but with an eventual healthier stability and openness. It forces a reflection and debate on how we do business by pushing things into the public sphere. Unfortunately, the release of classified information also creates fear among those in power and security experts. This can have a contrary effect to the one desired, with more secrecy and a race for improved protection mechanisms, which hackers will again circumvent, and so on.

Information needs to be 'liberated' for people to be and stay free. Hackers may very well be our "freedom of information fighters," by continually staying ahead of the game in the race for protective measures. It is part of their social role – they commit illegal acts that destabilizes, but at the same time their actions play an important role in keeping and improving transparency. Clearly here we are not talking about hackers that cause all sorts of mayhem for citizens, for instance by stealing their personal information. In an open world, there must still be room for privacy and confidentiality – for instance, privacy of personal information and confidentiality during criminal investigations. Openness does not mean free-for-all information chaos.

4. Technologies to End Secrecy?

The last question I would like to raise is whether technologies of the future may pose a definitive challenge for secrecy? One such technology is Artificial Intelligence (AI). Although advances in this field have been much slower than initially anticipated (Lungarella et al., 2007), progress has been made in the last decade with statistical methods that make sense of large amount of data and self-replicating self-adapting software agents that can attack networks (Kotenko, 2003). It is only conjecture at this moment, but one can imagine millions of intelligent programs scouting the world communication infrastructure and information systems for classified information. They would act as today's human hackers, but work on a much larger scale and incredibly faster. It may be difficult to keep information secret under the constantly adapting attacks. Certainly, there would be similar electronic counter-measures to stop intrusions.

Yet, the amount of information that could automatically be freed, analysed and organized for citizen's consumption (and foreign intelligence services!) might dwarf what we have seen in recent years. This may change our view of secrecy, in fact putting in question the very culture of hiding information in the first place if it has a high likelihood of being accessed anyway. Even encrypted information may not be immune the technological developments. Quantum computing could revolutionize current limits in processing speed, making code-breaking a simple matter (Iannotta, 2012; Politi et al., 2009).

References

Orlikowski WJ (1992), "The duality of technology: Rethinking the concept of technology in organisations", Organization Science, vol 3 (3) pp 398-427.

McLuhan M and Lapham LH (1994), LH. Understanding Media: The Extensions of Man. The MIT Press.

Smith MR and Marx L (1994), Does Technology Drive History? The Dilemma of Technological Determinism. Cambridge, MA and London: MIT Press. Pp. 280.

Postman, N (1993), Technopoly: The Surrender of Culture to Technology. New York: Vintage

Winston B. (1998) Media Technology and Society, A History From the Telegraph to the Internet (Routledge)

Harris P and Sarewitz D (2012) Destructive Creation and the New World Disorder, Current History 111(741) pp. 29

Feenberg, A (2004), "Democratic Rationalization". Readings in the Philosophy of Technology. David M. Kaplan. Oxford: Rowman & Littlefield, pp. 209-225

Kranzberg, M (1986) Technology and History: "Kranzberg's Laws", Technology and Culture, Vol. 27, No. 3, pp. 544-560

Best ML, Long WJ, Etherton J, and Smyth T (2011) Rich digital media as a tool in post-conflict truth and reconciliation. Media, War & Conflict December 4: 231-249

Levy, S (1984) Hackers: Heroes of the Computer Revolution. Nerraw Manijaime/Doubleday (New York)

Lungarella M, Iida F, Bongard JC, and Pfeifer R. (2007). AI in the 21st century - with historical reflections. In 50 years of artificial intelligence, Max Lungarella, Rolf Pfeifer, Fumiya Iida, and Josh Bongard (Eds.). Lecture Notes In Computer Science, Vol. 4850. Springer-Verlag, Berlin, Heidelberg 1-8.

Politi A, Matthews JCF, and O'Brien JL (2009) Shor's Quantum Factoring Algorithm on a Photonic Chip Science 4 September 2009: 325

Iannotta B (2012) Quantum Computing Could Bust Secret Codes — Someday C4ISR Report Nov. 8, 2012

Kotenko I. (2003). Teamwork of hackers-agents: modeling and simulation of coordinated distributed attacks on computer networks. In Proceedings of the 3rd Central and Eastern European conference on Multi-agent systems (CEEMAS'03), Vladimír Mařík, Michal Pechouček, and Jörg Müller (Eds.). Springer-Verlag, Berlin, Heidelberg, 464-474.

Kamar E, Hacker S, and Horvitz E. (2012). Combining human and machine intelligence in large-scale crowdsourcing. In Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems - Volume 1 (AAMAS '12), Vol. 1. International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 467-474.