SOCIETY FOR PHILOSOPHY AND TECHNOLOGY
Technology in the Age of Information
18th International Conference of the Society for Philosophy and Technology
ISEG, Technical University of Lisbon, Portugal
July 4-6, 2013

Location: Anf. BES (Q)
3.30-5pm
5 July 2013
15 min talk (5 mins questions)

<Slide 1>

Understanding Cybersecurity: Ethical and Conceptual Considerations

Abstract

In this paper I provide an ethical and conceptual analysis of the emerging concern with 'cybersecurity.' My paper provides an opportunity to explore some key concepts relating to security in the 'cyberrealm,' where kinetic and informational threats are rapidly converging. I offer a way of clearing the conceptual space relating to cybersecurity by exploring both how the term is being used and how it can be used.

First of all, I outline how cybersecurity (the systemised protection of individuals and states against cyberwarfare, cyberterrorism and cybercrime) is an increasingly prominent feature of the national security agenda. National governments, for instance, are becoming increasingly alarmed at the potential for serious attacks on cybersecurity and are responding accordingly. The Australian Government nominated 'malicious cyber attacks' as one of seven key national security risks in the recently released national security strategy and announced a new cybersecurity centre. And the U.S. Defense Department is set to more than quadruple its cyber forces over the next few years, in an effort to better protect critical networks and improve capacity for offensive cyber operations.

Next I argue that an effective cybersecurity strategy requires clarification of certain key concepts. An effective response to emerging threats to

cybersecurity requires a comprehensive understanding of the problem and its potential solutions. In particular, I argue, that it is an important task to establish a firm conceptual grasp on what we mean by the term 'cybersecurity' since many of the important conceptual aspects of cybersecurity remain unexamined. As a consequence, different people might be referring to different things when they discuss cybersecurity. A more conceptually rigorous approach to 'cybersecurity' will also help us to understand how the term should be used.

Then, to demonstrate my point that clarifying the meaning of cybersecurity is an important task, I provide an analysis of the ethics of surveillance as it applies to different aspects of cybersecurity. The permissibility of surveillance depends on how we conceive of cybersecurity in terms of cyberwarfare, cyberterrorism, and cybercrime. Key to any aspect of security is the ability to anticipate threats and construct both passive (i.e. building defences) and active (i.e. neutralising threats) solutions. Anticipation in the cyberworld requires surveillance. Yet surveillance infringes on the rights of individuals and exposes security practices to internal threats. Furthermore, as a second example, I demonstrate that distinguishing between cyberwarfare, cyberterrorism, and cybercrime is an important policy issue because it helps determine which institutional mechanisms to use on a particular security threat, a problem which is increasingly compounded by changing understandings of war, terrorism, and criminality.

Finally, I go on to consider two potential avenues for improving the conceptual clarity of cybersecurity. First, I examine cybersecurity in reference to the actor using the term. This approach considers how the term is used by a variety of actors with responsibilities for cybersecurity, including: IT professionals; government; military; police; private business and so on. Second, I examine cybersecurity in reference to the threat it describes. By providing a conceptual analysis of cybersecurity in terms of threat, the current and future technological and social developments that bear on cybersecurity practices can be systematically identified and analysed.

Introduction

In this paper, I provide an ethical and conceptual analysis of the emerging concern with ‘cybersecurity.’

<Slide 2>

First, I start out by briefly describing some key issues relating to security in the ‘cyberrealm,’ where kinetic and informational threats are rapidly converging. I presuppose a state-centric view of cybersecurity. By this I mean that the goal of cybersecurity is to protect national cyber-infrastructure.

Next, I outline the three types of cyberthreats to national cybersecurity: cyberwar, cybercrime and cyberespionage. I examine the argument that misunderstanding the nature of such cyber-threats creates a risk of escalating conflict.

Then, I touch on a second important moral question for national cybersecurity which is the concern that surveillance conducted for the purposes of security intelligence necessarily violates the right to privacy.

A. National Cybersecurity: Its importance and key concepts

<Slide 3>

First of all, cybersecurity is an increasingly prominent feature of the national security agenda.

National governments are alarmed at the potential for serious attacks on cybersecurity and are responding accordingly. The Australian Government, for instance, nominated ‘malicious cyber attacks’ as one of seven key national security risks in the recently released national security strategy.

And the U.S. Defense Department is set to more than quadruple its cyber forces over the next few years, in an effort to better protect critical networks and improve capacity for offensive cyber operations.

Given such an emphasis on cybersecurity, and the significant investment governments are making in this area, clearly it is an important task to establish a firm conceptual grasp on what we mean by the term 'cybersecurity.'

After all, it appears that Cybersecurity is being used in a very broad sense to capture everything that is happening in the cyber domain.

In this sense, cybersecurity is "an ill-defined catch-all for the nuanced problems of a tech-rich, hyper-networked world."[1]

Many states have national Cybersecurity centres to coordinate government policy on this issue. As mentioned above, Australia is in the process of setting up the Australian Cyber Security Centre (ACSC).

<Slide 4>

But Cybersecurity can also be used in a more specific sense as protecting national cyber-infrastructure from threats to its reliability. Admittedly, this is a state-centric view of cybersecurity.

One might talk about cybersecurity, for example, in terms of: 1) protecting the infosphere from attack (e.g. Taddeo); or 2) in terms of, the debate surrounding securitisation (e.g. Hansen & Nissenbaum, 2009).

Certainly, cybersecurity encompasses a range of conceptual axes: private and public infrastructure; threats against information or harms to or through physical devices.

But in this paper I stick with the state-centric perspective for the following two reasons:

First, State's are still key players in the cyberrealm.

Second, national security is an important area of academic research in its own right.

[1] Joshua Kopstein, "'Cybersecurity': how do you protect something you can't define?," The Verge, http://www.theverge.com/policy/2012/8/22/3258061/defining-cybersecurity-fud-cispa-privacy.

B. The risk of escalation

<Slide 5>

The range of cyberthreats to national security are complex and diverse. Cyberthreats may be isolated to single machines, distributed attacks against large numbers of machines at once, or mimetic in nature, such as computer viruses and worms.

Cyberthreats can be personal in nature (such as identity fraud) or could lead to massive and widespread harms (such as attacks on critical infrastructure). The intersections between these different types of cyberthreats create a startling number of requirements to secure against malevolent actors in cyberspace.

One important moral concern lies in the distinguishing between different types of national cybersecurity threats. These are, broadly speaking: cyberwar, cybercrime and cyberespionage.

According to Randall Dipert in his (2010) article "The Ethics of Cyberwarfare,"[1] **cyberwar** is the first major new form of warfare since the development of nuclear weapons. Cyberwarfare, in being compared to kinetic attacks, is then typically thought of in militaristic terms.

Yet expert actors operating from cyberspace do not need the support of a military institution to potentially do significant amounts of damage to national information networks or infrastructure.

In most cases, cyberthreats are more mundane than ruining power supplies or hijacking drones. Most cyberthreats are best described as **cybercrime**. These include: spam rings, extortion, money laundering, and other organized criminal activity.

For these threats, law enforcement is the more appropriate paradigm for conceptualizing cybersecurity; and this involves different actors with different reach, jurisdictional boundaries, and purposes.

Furthermore, cyberattacks might belong to a larger category of state-sponsored attacks on information systems. According to Dipert, "Such attacks include traditional counterespionage and disinformation campaigns, old-fashioned destruction of telephone lines, jamming of radio signals, killing of carrier pigeons, and so on."[2]

He goes on to suggest, that espionage is not usually an activity that has been considered part of the moral considerations in regard to conventional conceptions of Just War Theory. The ethical considerations in espionage and other intelligence-gathering operations are but one of the several traditionally neglected aspects within the morality of conflict (despite the growing interest in this field).[3]

<Slide 6>

In a recent article in "The National Interest" (13 May), Pano Yannakageorgeos argues that even experienced professionals all too often confuse cybercrime and espionage with cyber warfare. According to Yannakageorgeos it is "increasingly important that discussions of malicious cyber activities are accurately described" since "there is always a risk of escalating a case of espionage or crime to international armed conflict."[2]

In other words, we don't want states overreacting to cyber-threats.

The key mistake here is to conflate an attack using a "cyber-weapon" with one that involves "cyber-exploitation."

Cyberweapons are software used to attack other software (or data within computer systems) with the intention of doing damage. Cyberweapons damage software in a variety of ways. But this damage to software also has the potential to harm physical infrastructure and humans.

There are, however, also non-damaging cyber-attacks which aim to exploit an information system without damaging it. Examples include: 1) theft of information (both state-sponsored and criminal); 2) creating

[2] Panayotis A. Yannakogeorgos, "Keep Cyberwar Narrow," The National Interest, http://nationalinterest.org/commentary/keep-cyberwar-narrow-8459.

unauthorised access (or a back door) to a system; or 3) attempts to take control of the information system.

The important point here is that we should acknowledge an important distinction between "cyberweapons" (which aim to damage national cyber-infrastructure) and "cyber-exploitation" (which involves a non-damaging "attack" on national cyber-infrastructure), and then respond accordingly.

C. Surveillance and national security

<Slide 7>

A second important moral concern in national cybersecurity is with surveillance conducted for the purposes of collecting security intelligence.

National security intelligence is the intelligence collected, analysed and disseminated for decision-makers in the support of the security of the state.

Key to any aspect of security is the ability to **anticipate threats** and construct both passive and active solutions (i.e. building defences and neutralising threats).

Anticipation in the cyberrealm requires surveillance. Yet surveillance infringes on the rights of individuals and exposes security practices to internal threats.

Recent events have brought to light concerns "over the growing ability and tendency of intelligence and security services to intercept, monitor, and retain personal data in an increasingly cyber-dependent world."[3]

And these concerns are not new. "The 2009 UK House of Lords report, *Surveillance: Citizens and the State*, highlighted significant concerns regarding the possible threat that surveillance practices pose to individual privacy. The report sought to stress the need to review CCTV

[3] Ross Bellaby, "What's the Harm? The Ethics of Intelligence Collection," *Intelligence and National Security* 27, no. 1 (2012): 94.

camera usage, internet traffic monitoring, DNA databases and wiretaps, questioning the role they should have in a western liberal society."[4]

<Slide 8>

Clearly, it is not viable for intelligence agencies to maintain a continued shadowy existence, free to act out of sight and out of mind.[5]

As Ross Bellaby pointed out in his 2010 article "What's the Harm? The Ethics of Intelligence Collection, there is a tension between the belief that:

1) 'there are aspects of the intelligence business, as practised by all major countries, that seem notably disreputable',

2) 'without secret intelligence we will not understand sufficiently the nature of some important threats that face us';

3) political leaders have an ethical obligation to act so as to protect their people since in the words of Thomas Hobbes, 'Princes are obliged by the law of nature to make every effort to secure the citizens' safety . . . they may not do otherwise.'

4) And as a result, intelligence agencies face a tension created by, on the one hand, the duty to protect the political community and, on the other hand, the reality that intelligence collection may entail activities that negatively affect individuals."[6]

There is, however, an important distinction between vacuuming up all available data for analysis when compared with targeted intelligence collection for the purposes of security. Targeted collection might be morally justified in some cases. In contrast, the indiscriminate collection of data is not proven to be effective.

[4] Ibid.

[5] Ibid., 95.

[6] Ibid.

As Kenneth Roth recently suggested, “Recognizing a privacy interest in our metadata would not undermine efforts to fight terrorism. In recent weeks, spokesmen for the NSA have claimed that the surveillance operations revealed by Edward Snowden have disrupted dozens of terrorist plots. Upon scrutiny, however, many of these plots appear in fact to have been uncovered not because of the mass collection of our metadata but through more traditional surveillance of particular phone numbers or email addresses”[7]

In short, the focus of cybersecurity should be on the means of protecting the moral rights of individuals as well as the prevention (or just prosecution) of wars between states.

This inclusive approach to national security more accurately tracks the way in which national security intelligence has evolved and responded to circumstances following the end of the Second World War from a preoccupation with fighting or preventing wars between states to currently supporting a broader human security agenda.[8]

Conclusion

<Slide 9>

In conclusion, distinguishing between cyberwarfare, cyberespionage, and cybercrime is an important ethical and conceptual issue because it helps determine which institutional mechanisms to use on a particular security threat, a problem which is increasingly compounded by changing understandings of war, terrorism, and criminality.

What is required, in particular, is to determine the specific institutional responsibilities for national cybersecurity, including military, law enforcement, and intelligence aspects.

Importantly, a focus on national security is not incommensurable with the promotion of human security and we should be concerned with both.

[7] Kenneth Roth, "Rethinking Surveillance," The New York Review of Books, http://www.nybooks.com/blogs/nyrblog/2013/jul/02/electronic-surveillance-missing-laws/.

[8] Patrick F. Walsh, *Intelligence and Intelligence Analysis* (New York: Routledge, 2011). 9-10.

OTHER POTENTIAL POINTS

An important concern in the collection of TECHINT for the purposes of protecting national security is with surveillance. Key to any aspect of national security is the ability to **anticipate threats** and construct both passive and active solutions (i.e. building defences and neutralising threats). Anticipating threats in national security requires surveillance. Yet surveillance infringes on the rights of individuals and exposes security practices to internal threats.

Recent events have brought to light concerns “over the growing ability and tendency of intelligence and security services to intercept, monitor, and retain personal data in an increasingly cyber-dependent world.”

And these concerns are not new. “The 2009 UK House of Lords report, *Surveillance: Citizens and the State*, highlighted significant concerns regarding the possible threat that surveillance practices pose to individual privacy. The report sought to stress the need to review CCTV camera usage, internet traffic monitoring, DNA databases and wiretaps, questioning the role they should have in a western liberal society.”

Clearly, it is not viable for intelligence agencies to maintain a continued shadowy existence, free to act out of sight and out of mind. As Ross Bellaby pointed out in his 2010 article "What's the Harm? The Ethics of Intelligence Collection,” there is a tension between the belief that:

1) ‘there are aspects of the intelligence business, as practised by all major countries, that seem notably disreputable’,

2) ‘without secret intelligence we will not understand sufficiently the nature of some important threats that face us’;

3) political leaders have an ethical obligation to act so as to protect their people since in the words of Thomas Hobbes, ‘Princes are obliged by the law of nature to make every effort to secure the citizens’ safety . . . they may not do otherwise.’

4) And as a result, intelligence agencies face a tension created by, on the one hand, the duty to protect the political community and, on the other hand, the reality that intelligence collection may entail activities that negatively affect individuals.”

There is, however, an important distinction between vacuuming up all available technical data for analysis when compared with targeted intelligence collection for the purposes of national security. Targeted collection might be morally justified in some cases. In contrast, the indiscriminate collection of data is neither justified nor proven to be effective.

As Kenneth Roth suggested, “Recognizing a privacy interest in our metadata would not undermine efforts to fight terrorism. In recent weeks, spokesmen for the NSA have claimed that the surveillance operations revealed by Edward Snowden have disrupted dozens of terrorist plots. Upon scrutiny, however, many of these plots appear in fact to have been uncovered not because of the mass collection of our metadata but through more traditional surveillance of particular phone numbers or email addresses”

In short, the focus of TECHINT collection should be on the means of protecting the moral rights of individuals as well as the prevention (or just prosecution) of wars between states.’

Ross Bellaby, "What's the Harm? The Ethics of Intelligence Collection," *Intelligence and National Security* 27, no. 1 (2012): 94.

Kenneth Roth, "Rethinking Surveillance," The New York Review of Books, http://www.nybooks.com/blogs/nyrblog/2013/jul/02/electronic-surveillance-missing-laws/.

Notes

Bellaby, Ross. "What's the Harm? The Ethics of Intelligence Collection." *Intelligence and National Security* 27, no. 1 (2012/02/01 2012): 93-117.

Dipert, Randall R. "The Ethics of Cyberwarfare." *Journal of Military Ethics* 9, no. 4 (2010/12/01 2010): 384-410.

Kopstein, Joshua. "'Cybersecurity': How Do You Protect Something You Can't Define?" The Verge, http://www.theverge.com/policy/2012/8/22/3258061/defining-cybersecurity-fud-cispa-privacy.

Roth, Kenneth. "Rethinking Surveillance." The New York Review of Books, http://www.nybooks.com/blogs/nyrblog/2013/jul/02/electronic-surveillance-missing-laws/.

Walsh, Patrick F. *Intelligence and Intelligence Analysis*. New York: Routledge, 2011.

Yannakogeorgos, Panayotis A. "Keep Cyberwar Narrow." The National Interest, http://nationalinterest.org/commentary/keep-cyberwar-narrow-8459.

[1] Randall R. Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9, no. 4 (2010): 385.

[2] ———, "The Ethics of Cyberwarfare," 386.

[3] Ibid., 389.