Hackers as Terrorists? Why it Doesn't Compute

Maura Conway

The bulk of this article is concerned with showing why computer hackers and terrorists are unlikely to form an unholy alliance to engage in so-called cyberterrorism. The remainder of the paper examines why neither hacktivists nor crackers fall easily into the cyberterrorist category either.

Introduction

'Hacking' is the term used to describe unauthorized access to or use of a computer system. The term 'hacktivism' is composed of the words 'hacking' and 'activism' and is the handle used to describe politically motivated hacking. 'Cracking' refers to hacking with a criminal intent; the term is composed of the words 'criminal' and 'hacking.' In a majority of both academic analyses and media reports of cyberterrorism, one or other of these terms – hacking, hacktivism, cracking – or the activities associated with them are equated with or identified as variants of cyberterrorism.

Hackers as terrorists?

Much has been made of the similarities between profiles of terrorists and those of hackers. Both groups tend to be composed primarily of young, disaffected, males. In the case of computer hackers, a distinct psychological discourse branding them the product of a pathological addiction to computers has emerged. In fact, a large number of hackers who have been tried before the criminal courts for their exploits have successfully used mental disturbance as a mitigating factor in their defence, and have received probation with counselling instead of jail time as a result. These young men have allowed themselves to be portrayed as personal and social failures: computer-dependent individuals, vulnerable to the personal and professional frustrations that have been found to underlie anti-social behaviour.

Terrorist groups to hire hackers?

Not likely

- Recruiting hackers for serious crime is more difficult than buying information for intelligence gathering.
- Contacting hackers could expose terrorists to operational security risks.
- Lack of IT expertise among a terrorist group could lead to the recruitment of inadequately skilled hackers.
- There is the risk that hired hackers would change sides for monetary gains.

Hackers are commonly depicted as socially isolated and lacking in communication skills. Their alleged anger at authority is said to reduce the likelihood of their dealing with these frustrations directly and constructively. In addition, the flexibility of their ethical systems; lack of loyalty to individuals, institutions, and countries; and lack of empathy for others are said to reduce inhibitions against potentially damaging acts. At the same time, their description as lonely, socially naïve, and egotistical appears to make them vulnerable to manipulation and exploitation.

Hackers for hire

Recently, the possibility of terrorist groups employing the services of hackers to carry out attacks has received growing attention.

Some hackers have demonstrated a willingness to sell their skills to outsiders. The most famous example is the Hanover Hackers case. In 1986, a group of hackers in Hanover, Germany, began selling information they obtained through unlawfully accessing the computer systems of various Departments of Energy and Defence, a number of defence contractors, and the US Space Agency NASA, to the Soviet KGB. Their activities were discovered in 1988; two years later the group were finally identified and apprehended.[1] In the early 1990s, a group of Dutch hackers succeeded in accessing US Army, Navy, and Air Force systems. They sought to sell their skills and sensitive information they had obtained via the intrusions to Iraq, but were apprehended by police in the Netherlands.

A majority of the analyses of hackers-for-hire stress the ease and advantages of such outsourcing. These analysts presume that terrorist groups will be able to easily contact hackers-for-hire, while keeping their direct involvement hidden through the use of cut-outs and proxies. The hackers could then be employed to reconnoitre enemy information systems to identify targets and methods of access. Furthermore, it is posited that if hacker groups could be employed to actually commit acts of cyberterrorism, terrorist groups would improve their ability to avoid culpability or blame altogether.

The drawbacks

There are important risks and disadvantages to such schemes, however. First, seeking to employ hackers to commit acts not just of disruption, but of significant destruction that may involve killing people would in all likelihood prove considerably more difficult than buying information for the purposes of intelligence gathering. Second, simply contacting, never mind employing, would-be hackers-for-hire would subject terrorists to significant operational security risks. It is notoriously difficult to confirm with any certainty with whom one is in contact in a purely virtual relationship. Third, terrorist organisations run the risk of

cyber-surrogates being turned into double agents by hostile governments or shadowy others. There is a strong case to be made for such hackers changing sides. This is because the primary motive of the hacker-for-hire is financial gain thus, given sufficient monetary inducement, such individuals are unlikely to object to reporting to other than their original 'employer.'

David Tucker of the Naval Postgraduate School in Monterey, California also has some interesting insights into the hacker-for-hire scenario. Based on a simulation in which he took part, which involved a hacker and members of a number of terrorist organizations, Tucker foresees potential organizational problems for any hacker-terrorist collaboration. He points out that on those occasions when hackers aren't acting alone, they operate in flat, open-ended associations. This is the opposite of many terrorist groups, which are closed hierarchical organizations. There is certainly the potential for clashes between these different organizational styles, developed in different operating environments, and derived from different psychological needs.

Tucker reports that a former member of ETA (Basque Homeland and Liberty) who was involved in the simulation repeatedly stressed the need to belong and the strength of attachment to the group as characteristic of members of clandestine organizations. This is not a character trait typically associated with hackers. In fact, in the simulation in which Tucker took part, the hacker and the terrorists involved disagreed over tactics and had difficulty communicating. Eventually, these difficulties became so great that it resulted in a breakdown in the simulation group. The hacker and the terrorists were simply not able to work together. Tucker observes that if the breakdown can be generalised, it would have obvious consequences for hacker-terrorist collaboration.[2]

Another risk faced by terrorists planning to employ IT to carry out attacks arises when the terrorists themselves lack sufficient computer expertise: there is the likelihood that they would recruit hackers who would prove insufficiently skilled to carry out the planned attacks.

Open source intelligence

O'Brien and Nusbaum make an interesting point when they assert that:

'As IT capabilities continue to proliferate, merging advances in computing with telecommunications and related technologies, both the amount of information and the types of information readily

available from open sources are greater than ever before. It is, therefore, ironic that, although there has been a great deal of theorising regarding the potential for terrorist groups to use [Information Warfare], there has been little open-source research on this subject. Open source intelligence (OSINT) is definitely a key asset for monitoring potential threats by cyberterrorists, especially as information concerning Western IT programmes, weaknesses and vulnerabilities can easily be drawn from open sources.'[3]

The likely scenario is cyberattacks carried out by terrorists with hacking skills

O'Brien and Nusbaum suggest that intelligence agencies should utilise online chat forums, hacker websites, etc. to gather intelligence on contemporary asymmetric threats. They suggest that most hackers possess a large degree of hubris with regards to their hacking knowledge and abilities as a result of which such "threat-savvy users" could be coaxed into revealing vulnerabilities they had discovered on the Net, as well as boasting about their own abilities and exploits. This position is endorsed by Soo Hoo, Goodman, and Greenberg:

'Foreign Bases of operation might be useful for intelligence-gathering activities, but again, they are not required for IT-enabled terrorism…[I]nformation about various systems' vulnerabilities is often shared online between hackers on computer bulletin boards, websites, news groups and other forms of electronic association, and this information can be obtained without setting foot in the target country.'[4]

Cybermercenaries

It seems unlikely, however, that professional hackers or cyber mercenaries would engage in the cavalier behaviour described above:

While amateur hackers receive most publicity, the real threat are the professionals or 'cyber mercenaries.' This term refers to highly skilled and trained products of government agencies or corporate intelligence branches that work on the open market.

The Colombian drug cartels hired cyber mercenaries to install and run a sophisticated secure communications system; Amsterdam-based gangs used professional hackers to monitor and disrupt the communications and information systems of police surveillance teams.[5]

There is no evidence of such mercenaries having carried out attacks under the auspices of known terrorist organizations, however.

Alternatives?

The only likely scenario, given the above, is cyber attacks carried out by terrorists with hacking skills. This is not impossible. The current trend towards easier-to-use hacking tools indicates that this hurdle will not be as high in the future as it is today, even as it is significantly lower today than it was even two or three years ago. According to William Church, a former US Army Intelligence Officer, the IRA (Irish Republican Army) were on the verge of carrying out such attacks, prior to the Northern Ireland peace process.

They had computer-oriented cells. They could have done it. They were already attacking the infrastructure by placing real or phoney bombs in electric plants, to see if they could turn off the lights in London. But they were still liking the feel of physical weapons, and trusting them.[6]

This is unsurprising: terrorists are generally conservative in the adoption

of new tools and tactics. Factors influencing the adoption of some new tool or technology include the terrorist group's knowledge and understanding of the tool, and their trust in it. Terrorists generally only put their trust in those tools that they have designed and built themselves, have experimented with, and thus know from experience will work. It's for this reason that weapons and tools generally proliferate from states to terrorists.

So much for hackers as cyberterrorists, but what of hacktivists?

Hacktivism versus cyberterrorism

Hacktivism grew out of hacker culture, although there was little evidence of sustained political engagement by hackers prior to the mid-1990s. 1998 is viewed by many as the year in which hacktivism really took off. It was in '98 that the US-based Electronic Disturbance Theatre (EDT) first employed it's FloodNet software in an effort to crash various Mexican Government websites to protest the treatment of indigenous peoples in Chiapas and support the actions of the Zapatista rebels. Over 8000 people participated in this, one of the first digital sit-ins. It was also in '98 that JF, a young British hacker, entered about 300 websites and replaced their home pages with anti-nuclear text and imagery. At that time, JF's hack was the biggest political hack of its kind. 'Hacktions' also took place in Australia, China, India, Portugal, Sweden, and elsewhere in the same year.[7] Michael Vatis, one-time Director of the FBI's National Infrastructure Protection Center (NIPC), has labelled such acts as cyberterrorism.

MVDA versus IVDA

Tim Jordan identifies two different types of hacktivism: Mass Virtual Direct Action (MVDA) and Individual Virtual Direct Action (IVDA). According to Jordan

'Mass Virtual Direct Action involves the simultaneous use, by many people, of the Internet to create electronic civil disobedience. It is named partly in homage to the dominant form of offline protest during the 1990s, non-violent direct action or NVDA'.[8]

The FloodNet attack on the Mexican Government websites described above was an example of MVDA as was the action against the 1999 World Trade Organisation (WTO) conference in Seattle. The organizers of the latter event, the UK-based Electrohippies, estimated that over 450 000 people participated in their sit-in on the WTO website. In contrast to MVDA, IVDA utilises classical hacker/cracker techniques and actions for attacking computer systems, but employs them for explicitly political purposes. Jordan makes the point that the name IVDA does not mean the actions are necessarily undertaken by those acting alone, but instead that the nature of such actions means that they must be taken by individuals (i.e. they in no way rely on mass action), although they may be taken by many individuals acting in concert.[9] JF's anti-nuclear protest described above was an example of IVDA, which generally consists of infiltration of targeted networks and semiotic attacks (i.e. website defacements).

> *Crime syndicates are more interested in having a functioning Internet than attacking it*

The major difference between MVDA and IVDA, apart from those already described, is that MVDA activists rarely seek to hide their identities – through the use of pseudonyms (handles), for example – or cover their tracks. Advocates of MVDA seek to gather together large groups of people to take part in hacktions and thus to inspire public debate and discussion, and maintain that they have a right to protest even if some of those protests are illegal or bordering on same. Many of those using IVDA, on the other hand, act alone and prefer to remain anonymous, which raises issues of representativeness, authenticity, etc. Finally, there are also differences between those hacktivists who are devoted to the classical hacking ideal of free flow of information and therefore view DoS attacks as wrong in principle and those who view MVDA as both direct non-violent action and important symbolic protest.[10]

Direct action net politics

It is the disruptive nature of hacktions that distinguishes this form of 'direct action Net politics' or 'electronic civil disobedience' from other forms of online political activism. Email petitions, political websites, discussion lists, and a vast array of other electronic tools have been widely adopted as recruitment, organization, lobbying, and communication techniques by social movements and political organizations of all sorts. This type of use of the Internet by political activists has been characterised as 'Computerised Activism.' The hacktivist movement is different, because it does not view the Internet simply as a channel for communication, but also crucially as a site for action. It is a movement united by its common method as opposed to its common purpose. Those political causes that have attracted hacktivist activity range from campaigns against globalization, restrictions on encryption technology, and political repression in Latin America to abortion, the spread of electronic surveillance techniques and environmental protection. Hacktivists are, therefore, arrayed across a far wider political spectrum than the techno-libertarian agenda with which committed 'netizens,' including the hacker fraternity, are often identified.

Cybercrime versus cyberterrorism

The issue of computer crime was first

raised in the 1960s, when it was realised that computers could easily be employed to commit a variety of frauds. Cyber crime is a more recent phenomenon, which was enabled with the introduction of the modem and the ability to remotely access computer systems, the explosion of E-commerce, and the resultant increase in financial transactions taking place via the Internet. Attempts to conflate cyberterrorism and cybercrime were inevitable. A UN manual on IT-related crime recognizes that, even after several years of debate among experts on just what constitutes cybercrime and what cyberterrorism, "there is no internationally recognized definition of those terms."[11] Nevertheless, it is clear that while cyberterrorism and cybercrime both employ information technology, their motives and goals do not coincide. Cybercriminals have financial gain as their primary motive. Areas in which individual criminals and criminal organizations have proven proficient in cyberspace include:

- Theft of electronic funds.
- Theft of credit card information.
- Extortion.
- Fraud.

Secondary to financial gain is the acquisition of information that can underpin the operations associated with making money. It is for this reason that transnational crime syndicates are probably more interested in maintaining a functioning Internet than attacking Internet infrastructures. In other words, organized crime groups view the Internet as a tool, not a target. This is because many such organizations employ the Internet – and the public telecommunications network generally – as a vehicle for intelligence gathering, fraud, extortion, and theft. For example, as banks and other financial institutions increasingly rely on the Internet for their daily operations, they become more attractive targets for criminal activity. Having said that, criminal groups, such as drug traffickers, may seek to penetrate information systems to disrupt law enforcement operations or collect information on operations planned against them.

Conclusion

Although the proceeds of cybercrime may be used to support terrorism, such activities ought not to be classed as cyberterrorism *per se*. Cracking is not cyberterrorism.

Hacktivists, although they use the Internet as a site for political action, are not cyberterrorists either. They view themselves as heirs to those who employ the tactics of trespass and blockade in the realm of real-world protest. They are, for the most part, engaged in disruption not destruction. According to Carmin Karasic, the software engineer who designed the FloodNet program: "This isn't cyberterrorism. It's more like conceptual art."[12]

Hackers are unlikely to become terrorists because their motives are divergent

The US Department of Justice labelled Kevin Mitnick, probably the world's most famous computer hacker, a "computer terrorist." On his arraignment, Mitnick was denied access not only to computers, but also to a phone, because the judge believed that, with a phone and a whistle, Mitnick could set off a nuclear attack. Incredulity aside, hackers are unlikely to become terrorists, because their motives are divergent. Despite the allegedly similar personality traits shared by both terrorists and present-day hackers, the fact remains that terrorism is an extreme and violent occupation, and far more aberrant than prankish hacking. Although hackers have demonstrated that they are willing to crash computer networks to cause functional paralysis and even significant financial loss, this propensity for expensive mischief is not sufficient evidence that they would be willing to jeopardise lives or even kill for a political cause.

References

1 For more, see Clifford Stoll's The Cuckoo's Egg. London: Pan Books (1991).
2 The Future of Armed Resistance: Cyberterror? Mass Destruction? (Conference Report). The Center on Terrorism and Irregular Warfare (2000).
3 Jane's Intelligence Review 15(11): 53.
4 Survival 39(3): 143.
5 Jane's Intelligence Review 15(10): 53.
6 Analyzing the Threat of Cyberterrorism TechWeb: The Business Technology Network 25 September 1998.
7 See "Hacktivists" of All Persuasions Take Their Struggle to the Web The New York Times 31 October 1998; The Golden Age of Hacktivism Wired 22 September 1998.
8 Computer Fraud & Security 2001(4):
9 Computer Fraud & Security 2001(4):
10 Computer Fraud & Security 2001(4):
11 Michael Mates Technology and Terrorism. Brussels: NATO (2001).
12 "Hacktivists" of All Persuasions Take Their Struggle to the Web The New York Times 31 October 1998.

About the author

Maura Conway is a PhD candidate in the Department of Political Science at Trinity College Dublin, Ireland, and a teaching fellow in the School of International Relations at the University of St. Andrews, Scotland. Her research interests are in the area of terrorism and the Internet. She has published in First Monday, Current History, the Journal of Information Warfare, and elsewhere.
School of International Relations
University of St. Andrews
Scotland Tel: +44 (0)1334 462939
Email: mc52@st-andrews.ac.uk