Threat Morphing in Cyberspace

https://www.e-ir.info/2010/03/08/threat-morphing-in-cyberspace-by-susan-w-brenner/

SUSAN W. BRENNER, MAR 8 2010

[1] Much has been written about cybercrime, cyberterrorism and cyberwarfare, but very little has been written about how, and why, these evolving threat categories differ from their real-world analogues. This is unfortunate, because the differences between the threat categories mean that the laws and strategies devised to deal with real-world threats are often ineffectual in dealing with cyber-mediated threats.

To understand why traditional tactics tend to be ineffectual in this context, we need to understand (i) the distinctions between real-world crime, terrorism and warfare and (ii) how and why cyberspace erodes these distinctions.

Criminal law is intended to maintain the baseline of order within a society that is essential for members of that society to carry out the activities essential for their survival and that of their society. A society cannot survive if its members are free to prey on each other in ways that undermine the critical level of order needed to fend off chaos.

Societies control crime by using two sets of rules: One is a set of civil rules that deals with status (e.g., when one is an adult, which adults have which rights), property, familial bonds and other critical matters. Some civil rules are informal norms; many take the form of laws, the enforcement of which falls to civil courts and civil litigation.

While civil rules suffice for other biological systems (e.g., ants, termites), humans have the capacity to deviate, i.e., to decide not to follow a civil rule; most of us do not disobey civil rules, but a subset of people are inevitably willing to do so. Societies use criminal rules to discourage conduct that seriously challenges a society's ability to maintain order. This criminal law is intended to keep potential rule-violators in line by letting the state sanction those who commit "crimes." A crime consists of someone's violating a law that forbids certain conduct or inflicting certain "harm."

So when Jane Doe murders John Doe, the society she belongs to will convict her of murder and impose a sanction, such as incarceration. The primary goal is to deter Jane from breaking more criminal rules; a secondary purpose is to deter others from following her example. The punishment imposed on Jane underscores the unacceptability of engaging in such conduct and presumably deters future rule-violation.

This system assumes that Individuals commit crimes. The assumption also applies to terrorism, which is essentially the commission of crime(s) for ideological reasons. Criminals commit crimes for financial reasons (e.g., fraud, theft) or passion (e.g., anger, sex). The motive for committing crimes is personal: I steal to benefit myself; I murder out of revenge. Terrorists commit crimes (e.g., killing people, damaging property) but for different reasons; terrorists commit crimes to promote an ideology.

Crime and terrorism both threaten internal order; both have historically been committed within the territory of a single nation-state. The internal character of crime and terrorism has been a function of necessity: In the real-world, it is physically impossible for me to steal property from someone located in another country; the constraints of geography and the historic limitations of travel meant that both crime and terrorism were therefore domestic threats which could be

War differs from crime and terrorism in two respects: One is that war is a struggle between collective entities; while it is waged by individuals, the players are the nation-states engaged in a political struggle. The primary reason why war

has been reserved for nation-states is that only they have been able to summon the resources (manpower, weapons) needed to wage war. The other difference is that unlike crime and terrorism, war threatens a society's ability to maintain external order — to fend off hostile nation-states and maintain a stable geographical and political environment.

Since societies have dealt with crime and warfare (and, to a lesser extent, terrorism) for millennia, they have developed rules – laws — that define each threat category and distinguish it from the other two. Societies also developed institutions that can deal effectively with crime and terrorism (law enforcement) and war (the military). The response authority of each is limited to the context within which a specific threat occurs: law enforcement deals with internal threats, the military deals with external threats.

Cyberspace erodes the distinctions between these three threat categories and, in so doing, erodes the efficacy of the institutions established to deal with each. It does so by undermining the validity of certain assumptions that underlie how we define and respond to the real-world threats.

Cyberspace eliminates the constraints of the physical world and geography becomes irrelevant; criminals can attack victims in other countries as easily as someone in their neighborhood. And while we have not yet seen a verified incident of cyberterrorism, the same is likely to be true of cyberterrorism, as well. This aspect of cybercrime and cyberterrorism means they are no longer purely internal threats; they can be internal or external threats or a mixture of both. And cyberspace erases identity; criminals can be anonymous or assume false identities. Both aspects of cybercrime and cyberterrorism erode the efficacy of the traditional law enforcement model, which assumes local crime, local criminals and a physical crime scene. The model's efficacy is further eroded by another characteristic of cybercrime and cyberterrorism: criminals can cause "harm" (criminal harm or terrorist harm) on a scale surpassing what is possible in the real-world because both activities can be automated. The increase in the scale of "harm" inflicted further challenges law enforcement because of the complexity of the conduct at issue (transnational commission plus a digital crime scene) and because it constitutes a new quantum of criminal activity added to the real-world crime with which law enforcement must continue to deal.

Cyberspace's eliminating the constraints of the physical world and reliable indicators of one's identity also impacts the institution we rely on to deal with external threats. In the physical world, war is unambiguous; when the Japanese attacked Pearl Harbor in 1941, there was no doubt this was war. The attackers wore uniforms and used airplanes and ships, all of which displayed the Japanese national insignia; that was one indicator this was war (attack by a nation-state, not individuals). Another indicator was the weaponry itself, which was far beyond the capacity of individuals to acquire and utilize.

We may – or may not – have seen instances of cyberwar. We know, though, that it will not require the use of sophisticated, expensive weapons that can only be utilized by nation-states. Like cybercrime and cyberterrorism, cyberwarfare will involve the use of digital signals – bits and bytes – which are available to anyone with a computer, Internet access and a minimal level of expertise.

This circumstance, combined with the effect cyberspace has on crime and terrorism, erodes the validity of the premises on which our threat categories are based. A cyberattack that comes (seems to come) from outside a nation-state's territory and is directed at what would be considered military targets may be cyberwar, but it might also be cybercrime or cyberterrorism. In cyberspace, states lose their monopoly on warfare and individuals lose their monopoly on crime and terrorism. Individuals can wage what is war in fact, if not in concept, and states can commit crimes and acts of terrorism.

This creates serious problems for countries that, like the United States, categorically bifurcate response authority into (i) civilian (crime/terrorism) and (ii) military (war). The bifurcation is predicated on the assumption that response personnel can quickly and easily distinguish crime/terrorism from war. That assumption is valid in the physical world, but is increasingly problematic for conduct vectored through cyberspace.

The challenge for nation-states – acting individually and/or collectively – is to factor the impact cyberspace has on the

traditional threat categories into their legal systems and into their threat response systems. The obvious option is to create a second tier of threats – a cyber-threat specific set of laws and response authorities. But while that option has an appealing simplicity, it probably is not the best approach because it could produce rule and institutional complexities that would hamper a nation-state's ability to respond to specific threat situations. In other words, hostile individuals might be able to exploit a dual-threat structure to their advantage.

Susan W. Brenner *is NCR Distinguished Professor of Law and Technology at the University of Dayton School of Law in Dayton, Ohio. She has spoken at numerous events, including two Interpol Conferences on Cybercrimes, the Middle East IT Security Conference, the American Bar Association's National Cybercrime Conference and the Yale Law School Conference on Cybercrime. She spoke on cyberthreats and the nation-state at the Department of Homeland Security's Global Cyber Security Conference and participated in a panel discussion of national security threats in cyberspace sponsored by the American Bar Association's Standing Committee on Law and National Security. She has also spoken at a NATO Workshop on Cyberterrorism in Bulgaria and on terrorists' use of the Internet at the American Society of International Law conference. Professor Brenner chaired a Working Group in an American Bar Association project that developed the ITU Toolkit for Cybercrime Legislation for the United Nation's International Telecommunications Union and has published many articles and two books on digital evidence, cybercrime and cyberthreats.*

[1]The analysis in this article is taken from Susan W. Brenner, *Cyberthreats: Emerging Fault Lines of the Nation-State* (New York: Oxford University Press 2009).