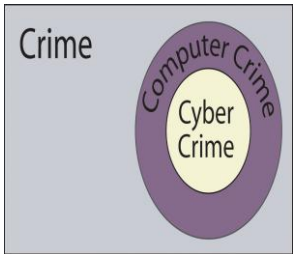
The Future of Cybercrime

Earl Moulton

Those of us in the Law Enforcement community have seen vast changes in our world in these past few years: changes in the demographics of our society, changes within our own agencies, and changes in the types and volumes of crime that we deal with, the kinds of suspects that commit those crimes and the victims that they create. Our legal environments have changed every bit as much as the physical environment that surrounds us. Given that state of flux, what can we possibly predict for the future that can have sufficient credibility to base our decisions on today?



One of the most significant changes has been the advent of cybercrime. While we may say that we know what it is when we see it, the term "cybercrime" has not been used with any degree of precision. For the purposes of this article, I will use "cybercrime" to mean "crime committed in relation to networked digital technology." To illustrate, it is helpful to think in terms of a Venn diagram.

Where all legislatively prohibited behaviour constitutes the complete set of crime, there is a subset which is committed in relation to digital technology. It is this subset which is more commonly described as "computer crime." A further subset is described where those digital technologies are linked in some manner so as to create a network. It is this ability to inter-connect, which I view as the *sine qua non* of cybercrime. For example, we can see that the keeping of a collection of child pornography on a standalone computer is both a crime and a computer crime. It only becomes a cybercrime when the computer storing the collection is connected to other computers and that connection is utilized to acquire, trade, sell, produce or otherwise deal with the pornographic images.

No matter where we are heading or how fast we're travelling, it is possible to get a sense of our direction and of our velocity by looking in the rear view mirror. What does our recent past tell us about that direction and velocity? Veteran cybernauts will recall that in 1996, less than a mere decade ago, there were approximately 16 million Internet users in the world. That number grew to 513 million by 2001 and is now thought to be about 650 million. Recall, too, that the '80's and early '90's were characterized by standalone personal computers, both in the workplace and at home. The growth since then of the Internet has been matched by the intranets that are equally ubiquitous at work and, increasingly, in the home and home-office environments. The mid-'90's also saw a somewhat brief discussion, now seemingly quaint, whether there really ought to be a "dot-com" domain on the Net and what constraints should be placed on it. As we move into the 21st century, the networked world continues to expand from wired to wireless. With convergence, telephony has become simply another aspect of our

interconnectedness.

Parallel to the changes in our network environment have come advances in the digital technology that we connect. In the '80's, we marvelled at the speed of our 8088 based machines working at 4.77 Megahertz, which we connected to local bulletin boards by means of 300 baud modems - but we could hit the "turbo" switch to get all the way up to eight Megahertz! Now we use three Gigahertz motherboards to connect via T1 lines to terabytes of storage and demand even better performance.

Simply stated we are travelling at ever greater speeds into an ever more networked world.

While looking in the rear view mirror has predictive value, extending the automotive analogy also tells us that looking in the rear view mirror is a very bad way to drive a car. Clearly, although informed by our past, our focus needs to be on the future. What might it hold?

The Macro Context

As we look down the road, we can make some well-founded guesses about where the road will go based on the topography we see before us. In the cybercrime context, that topography is determined by the interaction of changing technology and changing networks with the human side of our society. This is the topography that lies outside of the Venn diagram discussed above.

In society at large, there are some general themes that are very apparent and will have equally apparent impacts on cybercrime.

It is becoming a truism to say that digital technology has collapsed both time and distance. Both information and money now travel around the globe virtually instantaneously. What happens in Afghanistan is instantly known in Tokyo, causing comment in London and causing reaction in Washington. Just as significantly, that same information is reflected on the Hang Seng, the Bourse, and the New York Stock Exchange. And each of those is always "on" – connected 24/7. While law enforcement has always been 24/7, what is new today is that it is always rush hour somewhere.

In 1965, Moore's Law postulated data density will double about every 18 months. It is still true today. About every 18 months, one will get twice the memory and twice the speed from computers for the same price. With the advent of nanotechnology, there is absolutely no reason to believe that Moore's Law will cease to apply for the foreseeable future. The velocity that we perceived in the rear view mirror will continue. And recall, speed is distance over time while velocity includes acceleration. We are not just going faster, we're going faster *faster*.

Another aspect of general application is the demand by the general public for both greater transparency and greater accountability. For the Law Enforcement community, we see this in the increased levels of civilian oversight, in the demands for the disclosure of both the processes and the products of our investigations and, perhaps most apparently, on the nightly news. As technology enables greater and greater sharing of information, there will continue to be greater and greater

demands to act effectively and efficiently on that information. Those demands will make ever greater inroads on our resources and continue to reduce the resources available to prevent and investigate crime.

Finally, we need to consider an anti-intuitive outcome of the digital revolution. In *1984*, George Orwell posited a future entirely controlled by an omnipresent and seemingly omniscient government. That very compelling view is reflected in our latter day discussions of privacy and, in most prognostications, of the future. The reality, however, is entirely different. Rather than controlling more, governments actually control relatively much less. This is seen most notably with the Internet itself which continues to resist efforts by governments to control its content, reach and form. Indeed, one of the greatest challenges to the Department of Homeland Security is the fact that so much of today's critical infrastructure is held by private, corporate interests. Lessening even further the reach of governmental intervention are the twin realities that private interests are both transnational and often larger than governments themselves. The true Big Brother is not Big Government; it's Equifax. As a function, and as a creature, of government, the influence of the Law Enforcement community has been lessened to an equal degree.

The Specific Context

There are specific aspects of cybercrime about which we can make some educated guesses as to their likely role in the future.

Target Hardening

In the traditional crimefighting world, target hardening generally means making it more difficult for someone to commit a particular crime. It is also a maxim that things can never be made foolproof because fools are so ingenious. The same can be said of crooks. In the world of cybercrime, we see the introduction of new technologies and applications followed closely by criminals creating new scams taking advantage of those advances. Ultimately, security holes are plugged, business processes are changed and operating systems, protocols and applications are re-written, and the targets are 'hardened.' This modern day equivalent to the development of better bullets and better bullet-proofing is likely to continue - with the cybercops condemned to eternal second place in the race.

Two other facets of this race are of note. First, the length of time between the introduction of a new technology or application and someone taking criminal advantage is likely to decrease sharply. This phenomenon is already being seen in the virus arena. The time between the identification of a vulnerability and the release of an exploit has decreased dramatically in the past two years or so. The result has been the need to develop increasingly more sophisticated tools to deliver timely patches, and, thereby circumvents system administration ignorance and indolence. The second facet is that havoc wreaked on 'soft' targets before they can be 'hardened,' is likely to be much greater simply based on the sheer numbers of possible targets.

Nonetheless, we ought not to lose complete hope. We need only

recall the huge balloon of fraud that occurred shortly after the introduction of cell phones. Fairly quickly, however, there were technological responses and a more informed user cadre, and those levels of fraud returned to normal background levels. Tools to track offences occurring in P2P networks, over the IRC, and by 'spoofing' have become increasingly robust and offer a similar basis for optimism.

Anonymity

One of the contributors to cybercriminality is the anonymity that an Internet user experiences on the Net. While that anonymity is to some degree mythical, there is a very clear user ethos that holds that the use of the Net is, must be, should be, and need always be anonymous. Both our current experience of Internet use and broader social science experiments have shown that the perception of being anonymous lowers the barriers to criminal activity. Some have suggested that this may explain the otherwise unfathomable increases in child pornography activity. This "nobody will ever know that it's me" syndrome will only increase as the level of Internet use rises from its' current 10% worldwide level to levels approaching 50%.

Size of victim/suspect/target population

It is a concomitant of the rising participation level that the size of the possible victim population will also rise. So, too, will the absolute numbers of cybercriminals increase. What will the likely impact be on law enforcement? An answer to that question can be found in a reality that is all too often ignored. Early studies are showing that the profile of a typical cybercriminal is not at all like that of what we now think of as an ordinary criminal. We don't need statistical analysis of offender populations to tell law enforcement a truth we know from the streets - the levels of traditional crime are not falling off due to cybercrime. Bank robbers and burglars are not acquiring new skills sets to enter this new and exciting field. Cybercrime is an additional burden on law enforcement. Nothing in my experience as either a police officer or a futurist suggests that this is going to change.

There is special significance for raising the question of targets in addition to both victim and suspect populations. In the world of cybercrime, machines and devices controlled by individual victims are themselves separate targets. Where there used to be a single bank to be targeted by the bank robber, we now have automated teller machines located wherever there is a power source. Each of those machines are themselves targets for what they contain—cash—but also for the fact that they are avenues of access into banking networks and sources of access information—card and PIN information. Additionally, individuals now carry multiple targets. We have multiple, networked home computers, Web-enabled cell phones, Blackberrys, Palm devices, laptops, and cars communicating via satellites. Again, each of these target possibilities are in addition to existing targets and never simply replacing existing ones.

Timeliness

We considered briefly above the impact technology has had on the collapse of previous concepts of time.

This area, however, has special relevance to a number of specific aspects of cybercrime.

Fundamental to every criminal investigation is the acquisition of evidence. In the cybercrime world that evidence is exceedingly ephemeral. Network traffic logs, IP address assignments, random access memory, and Internet history files all pose special problems of timeliness. To the extent that current legal procedures, such as search warrants, require an inordinate amount of time to acquire and execute, the likelihood of evidence destruction, either deliberate or inadvertent, increases. When we layer an evidence request with the Mutual Legal Assistance Treaty process, the concept of timeliness loses all practical meaning.

Timeliness is also important to the identification of the *modus operandi* of a cybercrime. When thousands or millions of similarly situated possible victims exist, it becomes extremely important that the manner and means by which a cybercrime has been committed is discovered. That discovery must be then be made widely known to protect those possible victims.

Like traditional crime, much, if not most, cybercrime is committed for personal gain. Unlike traditional crime, the proceeds are not television sets, cash, or cars. Rather the proceeds of cybercrime are bits and bytes which, instantly, turn into credits in accounts, which get transferred into other accounts in other forms, in other institutions, in other countries, in other time zones, in other legal systems. The likelihood of ever extracting the profit from cybercrime becomes almost zero and raises the attractiveness of cybercrime in exact inverse proportion.

What is a Cybercrime 9-1-1?

In traditional policing, we all know how to priorize our calls for service. Just like with the media, 'if it bleeds, it leads.' If there is any risk of bodily harm occurring, the call goes to the top of the list. The same can be said of most budgeting processes. If there is a physically harmed victim involved, getting money into the policing budget to take action is seldom difficult. The final chapter in this phenomena is played out in sentencing proceedings in court. The sentencing of white collar criminals is notoriously lenient and can be understood in the absence of a bleeding victim. The experience to date suggests that cybercriminality is treated as simply another form of white collar crime and receives equally light sentences. Each of these implications compound themselves to make the future resourcing needs of law enforcement very difficult to meet.

There are many other aspects of cybercrime that will impact its future. Suffice to say at this point, that each of those factors leads to the inevitable conclusion that the challenge that will face the law enforcement community will be bigger, badder, more resource intensive, and more overwhelming than anything we have faced before.

Necessary Responses

If the situation is that critical, what can we do now to reduce the impact of cybercrime in the future?

One of the few things that has remained unchanged in the law enforcement world is the fundamental and essential importance of our human resources. This fact of life will not change. How, then, do we ensure that

our personnel have the necessary knowledge, skills, and abilities to cope with the cybercrime challenge? The likely answer lies in the same technology that poses the challenge. The use of computer-based training, distance learning, and the adoption of 'just-in-time' training models will all work to ensure that timely information gets into the proper hands. Some of these innovations will require changes in our institutional and educational mindsets. Nonetheless, initiatives such as the Canadian Police Knowledge Network are showing that there are real alternatives to simply sitting and wringing our hands in anguished worry.

It is also important to note that our new personnel come to us with a significantly different technological background than our existing personnel. For our new people, there is no such thing as a world without the Internet or 24/7 connectivity. They arrive on the job with skills and abilities that were not even dreamt of when we were recruited.

Dealing adequately with the challenge of cybercrime may also require the law enforcement world to modify what we consider to be our goal posts. For most agencies, success is marked by the arrest, prosecution and sentencing of an offender for an offence affecting one, or relatively few victims. In many cybercrimes, it may be more appropriate to place the emphasis on the determination of how a crime is committed and then taking the necessary prophylactic measures to prevent thousands, perhaps millions, of other victims being created. Such an approach might also address the existing difficulty in getting the corporate world to report cybercrime. Knowing that the primary focus is on cybercrime prevention and the proactive hardening of systems and processes would go a long way to alleviate current anxieties.

One reality that is shared by every agency that now supports a 'high tech' response capability is that these are very costly units to create and maintain. That phenomenon will not go away. We need to prepare our funding sources for a very significant and ongoing cost centre. The analogy that can be used is the different scale of funding that was required to move from riding horses to driving cars.

Finally, we need to apply a lesson from the traditional crime fighting arsenal. Crime rates for particular offence types really only change when there is fundamental change in the outlook of the general public. We need to educate the public about the 'dark places' on the Net. We need to get people to understand the importance of firewalls and secure passwords. We need an educated public to understand the risk to their private information and to their very identity that is posed by cyberspace. We need an informed and engaged public to demand, either as consumers or as an electorate, that industry supply the cyberworld equivalents of air bags and seat belts. It is that same electorate that will need to demand that laws be made effective and that artificial and archaic concepts of jurisdiction be removed.

As Sir Robert Peel understood centuries ago "the police are the public and the public are the police."

Some things don't change.