Cybercrime in the Year 2025

Gene Stephens

In 1981, this author wrote: “Data from all areas of the [criminal justice] system will be computerized and cross-referenced. Computers will store the *modus operandi* of convicted felons, and when a crime occurs, police may call on the computer to name the most likely suspects, or, in some cases, the exact offender” (Crime in the Year 2000, *The Futurist*, April 1981, p.52). It seemed quite logical at the time, but turned out to be overly optimistic, underestimating the antipathy to change and the turf protection within the system.

The first paragraph of a subsequent article was more on target: “Billions of dollars in losses have already been discovered. Billions more have gone undetected. Trillions will be stolen, most without detection, by the emerging master criminal of the twenty-first century—the cyberspace offender” (Crime in Cyberspace, *The Futurist*, Sept-Oct 1995, p. 24). Admittedly vague, it still seems to be a fairly accurate evaluation of the evolution of cybercrime.

In the same article, this author went on to correctly predict an explosion of cellular time theft and phone fraud; increased cyber attacks and fraud against the government and business; massive credit card theft and fraud; internal theft of identification of clients by financially-struggling and/or greedy employees of credit bureaus, banks, etc.; more cyber stalking and cyber porn, as well as cyber harassment and cyber vengeance; and use of biometrics and encryption as methods of protecting data in cyberspace.

In some other areas, forecasts weren’t as accurate. A fascination with the embryonic field of nanotechnology lead to a prediction of organic nanocomputers implanted in citizens’ brains by the early 21st century and thus forecasts of terrorists sending subliminal messages directly to the brain implants of potential recruits, cyber extortion by hacking into brain implants and scrambling or threatening to scramble information in it, and the problem of persons with brain implants being unable to separate virtual reality—perpetrated by cyber offenders—from flesh-and-blood reality. In defense, it’s still early 21st century—plenty of time for this technology and these disturbing crimes to begin to appear.

In the 1995 article, this author was rather pessimistic about the short-term capacity of police to cope with emerging cybercrime:

The outlook for curtailing cyberspace crime by technology or conventional law-enforcement methods is bleak. Most agencies do not have the personnel or the skills to cope with such offenses.... Cybercrime cannot be controlled by conventional methods. Technology is on the side of the cyberspace offender and motivation is high—it’s fun, exciting, and profitable (p. 28).

As far as a suggested solution:
The only real help is one that has not proven very successful in recent decades: conscience and personal values, the belief that theft, deception, and invasion of privacy are simply unacceptable (p. 28).

This approach could work, but unfortunately seems even more “pollyanna” today. So what can we expect in the next few years?

Technology Explosion

According to Ray Kurzweil’s “Law of Accelerating Returns,” technological change is exponential rather than linear; thus, “we won’t experience 100 years of progress in the 21st century—it will be more like 20,000 years of progress (at today’s rate)” (www.kurzweilai.net, published March 7, 2001). Predicting the advances and their impact on crime and crimefighting by 2025 then is analogous to reviewing the next 5,000 years of technological progress in society.

Kurzweil himself made several predictions that could have major impact in the field of cybercrime, such as that by 2010 PCs will be capable of answering questions by accessing information wirelessly via the Internet (one prediction that arrived a little early). By 2019, he held a $1,000 personal computer will have as much raw power as the human brain but possibly more important, computer chips will be everywhere, embedded in furniture, jewelry, walls, clothing, etc. Also by 2019, he predicted computers and humans would communicate via two-way speech and gestures rather than keyboards. Virtual sex, via computer, will become a reality, as education, business, and entertainment also will be increasingly computer based. Roadways, Kurzweil forecasts, will be automated and computer controlled, while human-robot relationships will be commonplace.[1]

Possibly the most renowned of Kurzweil’s predictions is the coming of “the singularity”—the melding of humans and machines. Kurzweil sees this process well underway by 2025, as nanobots begin to surf the human bloodstream on search and destroy missions to combat pathogens, and data nanobots augment human intelligence and access to information. Transhumans will be on their way to having within their bodies the capacity to communicate and interact with others—humans, machines, and transhumans.

As for this author’s forecasts, here goes: Computer/internet use will become increasingly seamless, as hands-free, voice-activated communications and data entry and retrieval will be commonplace by the early teen years of this new millennium. That will mean the world community has moved a long way in a few short years, as even in late 2007, when it was reported 1.25 billion people had access to the internet, only about 2% of the world population regularly accessed it (www.internetworldstats.com). Science fiction writer William Gibson, who coined the term “cyberspace” in his 1982 short story, “Burning Chrome,” forecasts a ubiquitous fully-wired world—a single unbroken interface without need for computers—will complete the evolution to full access of all citizens of earth. (www.williamgibsonbooks.com). [2]
Whereas the Defense Advanced Research Projects Agency (DARPA) set up the internet and set it in motion (www.arpa.mil), DARPA will likely overhaul its invention in the teen years, and not only will the outcome be faster and larger capacity usage, but by virtually “starting over” with the security aspects, the new internet will be safer and more difficult to attack and disable. [3]

Nanotechnology will increasingly impact cyberspace by the late teen years, and in trying to gain the most advantage possible from its use, new security gaps (which could turn into nightmares if not handled carefully) will emerge. For example, as data nanobots are implanted in the brain of users (later organic bots will become an integral part of the individual), special attention will have to be paid to providing advanced firewalls to keep intruders from cracking into the bots and terrorizing the recipient. Could there be a more frightening crime than having your brain-stored knowledge erased or scrambled, or hearing voices threatening to destroy your memory unless you pay extravagant blackmail—mindstalking? [4]

Designer nanobots may also be released on the worldwide web to engender types of mischief and destruction not yet contemplated. All advanced technology has the capacity to be used for good or evil, dependent on the developer/user, and nanotech would appear to be the ultimate example, as it literally can be used to develop nanosize weapons that could destroy the world while providing nanosize defense systems that could protect the planet.

The geometrically-enhanced capabilities of the emerging web technology spotlights the long-ignored issues of **who owns the worldwide web, who manages the worldwide web, and who has jurisdiction over the worldwide web?** The answer now is: nobody! Can the world’s most powerful socio-politico-economic network continue to operate almost at random, open to all, and thus excessively vulnerable to cyber criminals and terrorists alike? Yet any attempt to restrict or police the web can be expected to be met by extreme resistance from a plethora of users for a variety of reasons, many contradictory.

Another sound prediction would be that the internet will become not only the number one means of communicating, conducting business, socializing, entertaining, and just “living,” in the future but indeed will handle a huge majority of such interactions; thus failure to establish and enforce some basic ground rules will lead to socioeconomic disaster, at the very least.

If exchange of resources is to be accomplished almost exclusively over the internet, anonymous surfing will be a potential threat and moving funds without identification could perpetrate not only individual fraud but could bankrupt the system itself. Biometrics and more advanced systems of ID will need to be perfected to protect users and the network. In addition, multinational cybercrime units will be required to catch those preying on users worldwide, as web surfers in Arlington, Virginia, USA, and Victoria, British Columbia, Canada, may be victims of cyber scams perpetrated in
Cairo, Egypt, or Budapest, Hungary. Coordination and cooperation will be keys to making the internet a safer place to travel and conduct business.

As we near the year 2020—with its accumulation of 4,000 years equivalence of tech advancement from the beginning of the 21st century—it becomes more difficult to forecast, as even the concepts, theories, and formulae for the changes have not yet emerged from the plethora of ongoing research and development.

But again, here goes: Every square meter of atmosphere hugging the earth will be filled with unseen nano devices designed to provide seamless communication and surveillance among all persons in all places. Humans will already have nanoimplants to accommodate both the instant communications and identification capacity of the omnipresent network, with everyone on earth having a unique Internet Protocol (IP) address. Nano storage capacity being almost limitless, all activity and utterances will be recorded and recoverable. Transparency will become increasingly ubiquitous as word and deed—whether spoken or acted out in anger, frustration, or as a joke—can be almost instantly compared to “the record.” Can human or even transhuman behavior evolve rapidly enough to withstand such scrutiny? If current laws were enforced with this level of supporting evidence, who could pay for the prison space required to carry out the mandated punishment?

Another possibility would be the perfection of The Matrix—envisioned by Gibson and subject of a series of popular books and movies—where a powerful central force controls all activity in a seemingly free society. The reaction in individualistic societies, such as the U.S., would likely be similar to that in these fictional portrayals—rebellion with a goal of destruction of the web of control. A counter force that could create a different type of harm for the individual would be continuance of the policy of no control of the internet, allowing often destructive activity—e.g., harassment, terrorism and fraud—without jurisdiction and authority to curtail it. Which would be worse would depend on which value dominates—security (i.e., safety and order) or civil liberties (freedom and chaos). As always, the role of public safety in all this is finding the balancing point, where the degree of safety is enough to allow the pursuit of individual happiness.

Cybercrime Progression

As technology advances at a dizzying pace, so will the ways and means of those wishing to use the rapidly changing cyberspace as a tool/milieu for fun and profit or worse. In the immediate future, the increasingly creative scams to bilk internet users of their resources will continue, with literally scores of new schemes appearing daily on the worldwide web. Sheiks, abandoned Russian women, and unclaimed lottery winnings will be joined by relatives seeking heirs and other electronic “pigeon drops” yet unimagined.

For those who burn with faith or passion for a cause, the internet will continue to provide a means both to fleece infidels for funds to pursue their goals, while at the same time providing
an avenue for recruiting others to their flock, as well as presenting opportunities to target their enemies for economic and even physical destruction via cyber terrorism.

Already the number one crime in the U.S. and rapidly expanding throughout the internet world, identity theft can be expected to increase at a faster pace and wreak havoc on the financial and social worlds of millions around the globe. It well may be that the only way to gain control over this profitable criminal enterprise will be the suggested DARPA reconfiguration of the web and its security apparatus.

These, however, are short-term crises, which thanks to the rapid pace of change will be outmoded by the ubiquitous wireless communications network that should be fully evolved by the middle to late years of the second decade of this new millennium. What type of cybercrime will come with the absence of computers and only signals in the air to handle all social and economic activity is yet to be invented. Yet, unless a values revolution (whether spiritual, religious, or humanistic in origin) occurs and humans/transhumans choose to refrain from stealing, killing, and defiling one another, you can bet creative malcontents will develop new methods to manipulate the system for their own ends.

In its quest for speed and efficiency on the web, networks will grow in size and scope. For example, a network including all branches of a large bank becomes a larger net when several banks merge and larger still when all banks in a region join to reduce costs and speed service delivery. Then a national banking net emerges and is soon replaced by a multinational and finally a worldwide net. While the net becomes more powerful as it grows, it also becomes more vulnerable to attack. A shutdown of a regional net would create havoc, but the slack could be picked up by other nets. However, if the worldwide net is closed, true chaos ensues, leaving banks/customers at the mercy of blackmailers/extortionists/terrorists. Thus, the larger the networks (e.g., energy, medical, education; regional, international, worldwide), the more critical security becomes.

On the other hand, many may see a greater threat evolving from the powerful technology available to thwart cybercrime and, indeed, all criminal activity. Authorities have long said, “If you have nothing to hide, you have nothing to fear” when talking about police state surveillance capabilities. It would appear that theory will be well tested by the evolving technology of the next few years, as all activity will be seen and recorded and ready for retrieval and prosecution and then development of preventive strategies. Do we really want to live in a society where law is supreme, without recourse, and mistakes are not allowed, where “the record” is proof positive and there is no place for plea bargaining or mediation/arbitration. Have we evolved to this level of “perfection?”

Conclusion

The future path through cyberspace is filled with threats and opportunities, most of which cannot even be imagined at this time. With 5,000 years of technological progress
expected between 2100 and 2125, it's difficult to forecast the dilemmas that lie ahead, but thanks to the creativity and genius of William Gibson, Ray Kurzweil, and others like them, some predictions have been made and can be used as a base for an examination of future cybercrime and crimefighting.

The internet as we know it—computers, websites, email, blogs, commerce, etc.—may be outdated as soon as the early years of the next decade when a seamless, wireless network of airborne signals received directly by transmitters in the possession of individuals and nanobots implanted in the bodies of individuals handle all communication. At this point, cyber offenses will become very personal, as an attack on the web is a direct attack on the user—possibly even invading his brain and memory stored in neural networks.

As nanoscience advances to the point that bots in the atmosphere capture and record all spoken and physical activity, the choice will evolve: tightly control all human interaction by holding individuals responsible for every deed and action (each of which is supported by permanently stored evidence) in a efficiently networked worldwide web or allow creativity and individualism to emerge by refusing to set boundaries and jurisdictions on the internet, leaving it much as it is today—without management or enforcement. The former would curtail cybercrime and make the web a safe vehicle for communication, socializing, commerce, etc., but at a substantial cost to privacy, freedom of speech, and other civil liberties. The latter would allow a free flow of information and exchange of goods and services without government interference, but with a substantial threat to the economic and social lives of individuals and society itself posed by cyber offenders.

By 2025, it is likely the whole concept of the internet and cybercrime may be passé—part of the dustbin of history. The greatest threat then might be the extreme difficulty of separating virtual (cyber) reality from physical reality. Already psychologists warn that perception is more important than truth; thus, if cyber reality is more convincing than physical reality, does the virtual world become the “real” world? Welcome to The Matrix.

Notes


[2] In addition to a brief review of his life and works, partially in his own words, at Gibson’s “official website,” www.williamgibsonbooks.com, a more complete listing of his full body of work can be found at www.skierpage.com/gibson/biblio.htm.

Cybercrime is a crime that involves a computer and a network.[1][2] The computer may have been used in the commission of a crime, or it may be the target.[3] Cybercrime may harm someone's security and financial health.[4] There are many privacy concerns surrounding Cybercrime when confidential information is intercepted or disclosed, lawfully or otherwise. Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud in the US.[9] In 2018, a study by the Center for Strategic and International Studies (CSIS), in partnership with McAfee, concludes that nearly one percent of global GDP, close to $600 billion, is lost to cybercrime each year.[10] The World Economic Forum 2020 Global. Cyber-attacks and cybercrime continue to rise. Security threats are also becoming more complex: they feed on the ability to work cross-border and on inter-connectivity; they exploit the blurring of the boundaries between the physical and digital world; they exploit vulnerable groups, social and economic divergences. Attacks can come at a moment's notice and may leave little or no trace; both state and non-state actors can deploy a variety of hybrid threats; and what happens outside the EU can have a critical impact on security inside the EU. It has highlighted the need to guarantee security both in the physical and digital environments. It has underlined the importance of open strategic autonomy for our supply chains in terms of critical products, services, infrastructures and technologies. 18, 2020 (GLOBE NEWSWIRE) -- Cybersecurity Ventures predicts global cybercrime costs will grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This prediction is part of a special report conducted by Cybersecurity Ventures and sponsored by INTRUSION, Inc. (NASDAQ: INTZ). According to a study conducted by cybersecurity company McAfee, all of these and much more may be possible by the year 2025. Analyzing data from more than 7,000 consumers across twelve countries, the study provides insights into how people see the integration of technology with their everyday lives within eleven years. However, the pervasiveness of technology also threatens to make us vulnerable in ways we can't imagine today. Fearing the future. People have just started to understand that their personal data is not some ethereal thing, said Brian Johnson, Intel futurist. Cybercrimes are projected to increase over the next few years, and the need for tools/professionals to tackle this problem will equally go up. However, having the tools to fight cybercrime is not enough to help; instead, the professionals who can carry out the service matter even more. Vision five: The center of focus for cyberattacks will come from our global supply chains. However, this is set to change in the coming years up to 2025, due to the adoption of cybersecurity solutions all over the world. More companies are adopting analytical techniques such as machine learning to help them deal with cybercrimes and threats. To prevent further damage from taking place, most of these companies opt to hire professionals to help.