

CHAPTER 1

Connected, Dependent, and Vulnerable

Technology . . . is a queer thing; it brings you great gifts with one hand and it stabs you in the back with the other.

CHARLES PERCY SNOW

Mat Honan's life looked pretty good on-screen: in one tab of his browser were pictures of his new baby girl; in another streamed the tweets from his thousands of Twitter followers. As a reporter for *Wired* magazine in San Francisco, he was living an urbane and connected life and was as up-to-date on technology as anyone. Still, he had no idea his entire digital world could be erased in just a few keystrokes. Then, one August day, it was. His photographs, e-mails, and much more all fell into the hands of a hacker. Stolen in just minutes by a teenager halfway around the world. Honan was an easy target. We all are.

Honan recalls the afternoon when everything fell apart. He was playing on the floor with his infant daughter when suddenly his iPhone powered down. Perhaps the battery had died. He was expecting an important call, so he plugged the phone into the outlet and rebooted. Rather than the usual start-up screen and apps, he saw a large white Apple logo and a multilingual welcome screen inviting him to set up his new phone. How odd.

Honan wasn't especially worried: he backed up his iPhone every night. His next step was perfectly obvious—log in to iCloud

and restore the phone and its data. Upon logging in to his Apple account, he was informed that his password, the one he was sure was correct, had been deemed wrong by the iCloud gods. Honan, an astute reporter for the world's preeminent technology magazine, had yet another trick up his sleeve. He would merely connect the iPhone to his laptop and restore his data from the hard drive on his local computer. What happened next made his heart sink.

As Honan powered up his Mac, he was greeted with a message from Apple's calendar program advising him his Gmail password was incorrect. Immediately thereafter, the face of his laptop—its beautiful screen—turned ashen gray and quit, as if it had died. The only thing visible on the screen was a prompt: please enter your four-digit password. Honan knew he had never set a password.

Honan ultimately learned that a hacker had gained access to his iCloud account, then used Apple's handy "find my phone" feature to locate all of the electronic devices in Honan's world. One by one, they were nuked. The hacker issued the "remote wipe" command, thereby erasing all of the data Honan had spent a lifetime accumulating. The first to fall was his iPhone, then his iPad. Last, but certainly not least, was his MacBook. In an instant, all of his data, including every baby picture he had taken during his daughter's first year of life, were destroyed. Gone too were the priceless photographic memories of his relatives who had long since died, vanquished into the ether by parties unknown.

Next to be obliterated was Honan's Google account. In the blink of an eye, the eight years of carefully curated Gmail messages were lost. Work conversations, notes, reminders, and memories wiped away with a click of a mouse. Finally, the hacker turned his intention to his ultimate target: Honan's Twitter handle, @Mat. Not only was the account taken over, but the attacker used it to send racist and homophobic rants in Honan's name to his thousands of followers.

In the aftermath of the online onslaught, Honan used his skills as an investigative reporter to piece together what had happened. He phoned Apple tech support in an effort to reclaim his iCloud account. After more than ninety minutes on the phone, Honan learned that "he" had just called thirty minutes prior to request his password be reset. As it turns out, the only information anybody

needed to change Honan's password was his billing address and the last four digits of his credit card number. Honan's address was readily available on the Whois Internet domain record he had created when he built his personal Web site. Even if it hadn't been, dozens of online services such as WhitePages.com and Spokeo would have provided it for free.

To ascertain the last four digits of Honan's credit card, the hacker guessed that Honan (like most of us) had an account on Amazon.com. He was correct. Armed with Honan's full name and his e-mail and mailing addresses, the culprit contacted Amazon and successfully manipulated a customer service rep so as to gain access to the required last four credit card digits. Those simple steps and nothing more turned Honan's life upside down. Although it didn't happen in this case, the hacker could have just as easily used the very same information to access and pilfer Honan's online bank and brokerage accounts.

The teenager who eventually came forward to take credit for the attack—Phobia, as he was known in hacking circles—claimed he was out to expose the vast security vulnerabilities of the Internet services we've come to rely on every day. Point made. Honan created a new Twitter account to communicate with his attacker. Phobia, using the @Mat account, agreed to follow Honan's new account, and now the two could direct message each other. Honan asked Phobia the single question that was burning on his mind: Why? Why would you do this to me? As it turns out, the near decade of lost data and memories was merely collateral damage.

Phobia's reply was chilling: "I honestly didn't have any heat towards you . . . I just liked your [Twitter] username." That was it. That's all it was ever about—a prized three-letter Twitter handle. A hacker thousands of miles away liked it and simply wanted it for himself.

The thought that somebody with no "heat" toward you can obliterate your digital life in a few keystrokes is absurd. When Honan's story appeared on the cover of *Wired* in December 2012, it garnered considerable attention . . . for a minute or two. A debate on how to better secure our everyday technologies ensued but, like so many Internet discussions, ultimately flamed out. Precious little has changed since Honan's trials and tribulations. We are still every bit

as vulnerable as Honan was then—and even more so as we ratchet up our dependency on hackable mobile and cloud-based applications.

As with most of us, Honan's various accounts were linked to one another in a self-referential web of purported digital trust: the same credit card number on an Apple profile and an Amazon account; an iCloud e-mail address that points back to Gmail. Each had information in common, including log-on credentials, credit card numbers, and passwords with all the data connected back to the same person. Honan's security protections amounted to nothing more than a digital Maginot Line—an overlapping house of cards that came tumbling down with the slightest pressure. All or most of the information needed to destroy his digital life, or yours, is readily available online to anybody who is the least bit devious or creative.

Progress and Peril in a Connected World

In a few years' time, with very little self-reflection, we've sprinted headlong from merely searching Google to relying on it for directions, calendars, address books, video, entertainment, voice mail, and telephone calls. One billion of us have posted our most intimate details on Facebook and willingly provided social networking graphs of our friends, family, and co-workers. We've downloaded billions of apps, and we rely on them to help us accomplish everything from banking and cooking to archiving baby pictures. We connect to the Internet via our laptops, mobile phones, iPads, TiVos, cable boxes, PS3s, Blu-rays, Nintendos, HDTVs, Roku, Xboxes, and Apple TVs.

The positive aspects of this technological evolution are manifest. Over the past hundred years, rapid advances in medical science mean that the average human life span has more than doubled and child mortality has plummeted by a factor of ten. Average per capita income adjusted for inflation around the world has tripled. Access to a high-quality education, so elusive to many for so long, is free today via Web sites such as the Khan Academy. And the mobile phone is singularly credited with leading to billions upon billions of dollars in direct economic development in nations around the globe.

The interconnectivity the Internet provides through its fundamental architecture means that disparate peoples from around the world can be brought together as never before. A woman in Chicago can play *Words with Friends* with a total stranger in the Netherlands. A physician in Bangalore, India, can remotely read and interpret the X-ray results of a patient in Boca Raton, Florida. A farmer in South Africa can use his mobile phone to access the same crop data as a PhD candidate at MIT. This interconnectedness is one of the Internet's greatest strengths, and as it grows in size, so too does the global network's power and utility. There is much to celebrate in our modern technological world.

While the advantages of the online world are well documented and frequently highlighted by those in the tech industry, there is also a downside to all of this interconnectivity.

Our electrical grids, air traffic control networks, fire department dispatch systems, and even the elevators at work are all critically dependent on computers. Each day, we plug more and more of our daily lives into the global information grid without pausing to ask what it all means. Mat Honan found out the hard way, as have thousands of others. But what should happen if and when the technological trappings of our modern society—the foundational tools upon which we are utterly dependent—all go away? What is humanity's backup plan? In fact, none exists.

The World Is Flat (and Wide Open)

For centuries, the Westphalian system of sovereign nation-states has prevailed in our world. It meant that countries were to be sovereign in their territory, with no role for outside authorities to meddle in a nation's domestic affairs. The Westphalian structure was preserved through a system of borders, armies, guards, gates, and guns. Controls could be implemented to limit both immigration and emigration of people from a national territory. Moreover, customs and inspection structures would be established to control the flow of goods across national boundaries. Yet as prescient as the signatories to the Treaty of Westphalia were in 1648, none of them foresaw Snapchat.

Though physical borders still matter, such divisions are much less clear in an online world. Bits and bytes flow freely from one country to the next without any border guards, immigration controls, or customs declarations to slow their transit. The traditional transnational barriers to crime faced by former generations of thieves, thugs, and convicts have been demolished in the online world, allowing unsavory individuals to freely enter and exit any virtual location they please.

Think about that and its implications for our security. Once upon a time, if criminals attempted to rob a bank in New York's Times Square, several things were considered to be self-evident. First and foremost, it was assumed that the perpetrators had entered a physical location within the boundaries of the NYPD's Midtown South Precinct. The bank robbery would have breached both New York State and U.S. federal law, and the NYPD and the FBI would share joint jurisdiction to investigate the matter. The victim (in this case the bank) was also colocated within the physical jurisdiction of the concerned law enforcement authorities, greatly simplifying their investigation. Attempts to solve the case would have been bolstered by physical evidence likely left behind at the scene of the crime by the bank robber, including fingerprints on a note handed to a teller and DNA on the counter he jumped over, and perhaps via the images of his own face visible on the bank's security camera system. In addition, the crime itself was subject to certain physical limitations. The dollar bills stolen would have had weight and mass, and only so many could be carried away. The piles of cash might also have had an embedded exploding dye pack to flag the suspect to the police. But in today's world, long-established, tried-and-true investigative givens, such as jurisdictional commonality and physical evidence—fundamental tools for authorities to solve crimes—often no longer exist.

Compare the Times Square heist scenario above with the infamous 1994 Internet bank robbery carried out by Vladimir Levin from his apartment in St. Petersburg, Russia. Levin, a computer programmer, was accused of hacking the accounts of several of Citibank's large corporate customers and making away with \$10.7 million. Collaborating with accomplices around the world,

Levin transferred large sums of cash to accounts in Finland, the United States, the Netherlands, Germany, and Israel.

Who had jurisdiction for this matter? Was it the police in the United States, where the victim (Citibank) was located? Was it the cops in St. Petersburg, where the suspect carried out the alleged offense? Or was jurisdiction held in Israel or Finland, perhaps, where the ill-gotten funds were electronically delivered to fraudulent accounts? Levin never physically entered the United States to commit the crime. He left no fingerprints or DNA and was never marked by an exploding dye pack. Importantly, he never needed to physically carry the thousands of pounds of cash out of the bank; it was all accomplished with a mouse and a keyboard. No need for a mask or sawed-off shotgun either; Levin merely hid behind his computer screen and used a circuitous virtual route to cover his digital tracks.

The nature of the Internet means that we are increasingly living in a borderless world. Today anybody, with good or ill intent, can virtually travel at the speed of light halfway around the planet. For criminals, this technology has been a boon, as they hop from one country to the next virtually hacking their way across the globe in an effort to frustrate police. Criminals have also learned how to protect themselves from being tracked online. A smart hacker would never directly initiate an attack against a bank in Brazil from his own apartment in France. Instead, he would route his attack from one compromised network to another, from France, to Turkey, to Saudi Arabia, toward his ultimate target in Brazil. This ability to country-hop, one of the Internet's greatest strengths, creates enormous jurisdictional and administrative problems for the police and is one of the main reasons why cyber-crime investigation is so challenging and often feckless. A police officer in Paris has no authority to make an arrest in São Paulo.

The Good Old Days of Cyber Crime

The nature of the cyber threat has changed dramatically over the past twenty-five years. In the early days of the personal computer,

hackers were mostly motivated by the "lulz," or laughs. They hacked computer systems just to prove that they could do it or to make a point. One of the very first computer viruses to infect IBM PCs was the Brain virus, created in 1986 by the brothers Amjad Farooq Alvi and Basit Farooq Alvi, aged twenty-four and seventeen, of Lahore, Pakistan. Their virus was intended to be innocuous, to stop others from pirating the software the brothers had spent years developing. Brain worked by infecting the boot sector of a floppy disk as a means of preventing its copying and allowed the brothers to track illegal copies of their own software. The brothers, upset that others were pirating their software without paying for it, included an ominous warning that appeared on infected users' screens:

Welcome to the Dungeon © 1986 Brain &
Amjads (pvt). BRAIN COMPUTER SERVICES 730
NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-
PAKISTAN PHONE: 430791,443248,280530.
Beware of this VIRUS . . . Contact us for
vaccination . . .

Their message is notable for several reasons. First, the brothers claimed to have copyrighted their virus, a ballsy move indeed. Even more strange was the fact that they included their address and phone numbers for users to contact the virus originators for "vaccination," or removal of the virus. Their reasoning for creating the virus seemed logical enough to Basit and Amjad, but what they hadn't realized was their creation had the capacity to replicate and spread and did so the old-fashioned way, through human beings' carrying around 5.25-inch floppy disks from computer to computer. Eventually, Brain had traveled the globe, introducing Basit and Amjad to the rest of the world.

Over time, hackers grew more ambitious—and more malicious. Our interconnection to one another via computer bulletin board services meant that digital viruses no longer needed to travel via a "sneakernet," carried by human beings on floppy disks, but rather could spread via modem over telephone lines through early online services such as CompuServe, Prodigy, EarthLink, and AOL. Newer viruses and Trojans such as Melissa (1999), ILOVEYOU

(2000), Code Red (2001), Slammer (2003), and Sasser (2004) could now infect Microsoft Windows computers around the world with ease, destroying the term papers, recipes, love letters, and company spreadsheets we had saved to our hard drives. Suddenly we all had skin in this game.

Computer "malware," a portmanteau combining the words "malicious" and "software," now comes in many forms, but all seek to damage, disrupt, steal from, or inflict some illegitimate or unauthorized action on a data system or network:

- Computer viruses propagate by inserting a copy of themselves into another program, just as a real-world virus infects an available biological host.
- Computer worms also cause damage, but do so as stand-alone software and do not require a host program to replicate.
- Trojans, named after the mythical wooden horse used by the Greeks to infiltrate Troy, often masquerade as legitimate pieces of software and are activated when a user is tricked into loading and executing the files on a targeted system. Trojans frequently create "back doors" that allow hackers to maintain persistent access to an infected system. Trojans do not reproduce by infecting other files per se, but rather spread by deceiving users into clicking on a file or opening an infected e-mail attachment.

Virus writers today recognize that the public is slowly (very slowly) beginning to get the message not to click on files sent by strangers. As a result, criminals have updated their tactics to create so-called drive-by downloads, which use malware to exploit vulnerabilities in computer scripting languages such as Java and ActiveX, languages commonly used by Internet Web browsers. The world has moved online, and hacking tools such as Internet Explorer, Firefox, and Safari makes sense for criminals, though the new modus operandi comes with a heavy cost for unsuspecting users. Researchers at Palo Alto Networks discovered that as much as 90 percent of modern malware is now spread via previously hacked popular Web

sites that serve up the computer infection the moment an unsuspecting visitor stops by the site. Many large companies, including Yahoo!, a major destination portal around the world, have had their Web sites hijacked by criminals and thus unknowingly poisoned their own customers who innocently stopped by to check sports scores or the latest stock market returns.

The Malware Explosion

Now it's not just about the "lulz" but for want of money, information, and power that hackers ply their trade. In the early twenty-first century, as criminals figured out ways to monetize their malicious software through identity theft and other techniques, the number of new viruses began to soar. By 2015, the volume had become astonishing. In 2010, the German research institute AV-Test had assessed that there were forty-nine million strains of computer malware in the wild. By 2011, the antivirus company McAfee reported it was identifying two million new pieces of malware every month. In the summer of 2013, the cyber-security firm Kaspersky Lab reported it identified and isolated nearly 200,000 new malware samples every single day.

Taking a cynical approach to these statistics and presuming that antivirus companies might be incentivized to overstate the problem that they were established to combat, one could be inclined to deflate the numbers dramatically, say by 50 or even 75 percent. Even so, that would still mean that fifty thousand new viruses were generated each and every day. Think about the tremendous research-and-development effort that would be required on a global scale to create that volume of uniquely coded malware.

As any business owner knows, R&D is an expensive proposition. As such, the return on investment (ROI) required to support international organized crime's ongoing illicit computer programming efforts must be vast. An independent study by the trusted Consumers Union, publisher of *Consumer Reports* magazine, seems to confirm the mounting impact of computer malware. A survey of its members in 2011 revealed that one-third of the households in the United States had experienced a malicious software infection in

the previous year, costing consumers a whopping \$2.3 billion annually. And that's just the people who realize they've been attacked.

The Security Illusion

Each year, consumers and businesses around the world put their faith in the computer security software industry to protect them from the burgeoning threat of computer malware. According to a study by the Gartner group, worldwide spending on security software totaled nearly \$20 billion in 2012 and is forecast to skyrocket to \$94 billion spent annually on cyber security by 2017.

Ask most individuals what to do about computer viruses, and their very first answer would be to use an antivirus product from a company like Symantec, McAfee, or Trend Micro. The response is instinctual from a public that has been trained well. While such tools might have proven useful in the past, they are rapidly losing their efficacy, and the statistics are deeply revealing. In December 2012, Researchers at Imperva, a data security research firm in Redwood Shores, California, and students at the Technion-Israel Institute of Technology decided to put the standard antivirus tools to the test. They collected eighty-two new computer viruses and ran the malware against the threat-detection engines of more than forty of the world's largest antivirus companies, including Microsoft, Symantec, McAfee, and Kaspersky Lab. The results: the initial threat-detection rate was only 5 percent, meaning that 95 percent of the malware went completely undetected. That also means the antivirus software you are running on your own computer is likely only catching 5 percent of the emerging threats targeting your machine. If your body's own immune system had a batting average like that, you would be dead in a matter of hours.

Months later, the behemoths of the security software industry eventually update their software, but of course by then it's often too late. The fact of the matter is that criminals and virus writers are completely out-innovating and outmaneuvering the antivirus industry established to protect us against these threats. Worse, the "time-to-detection rate"—that is, the amount of time it takes from the initial introduction of a piece of malware "in the wild"

to be uncovered—is growing. For example, in 2012 researchers at Kaspersky Lab in Moscow uncovered a highly complex piece of malware known as Flame that had been pilfering data from information systems around the world for more than five years before it was detected. Mikko Hypponen, the well-respected chief research officer at the computer security firm F-Secure, called Flame a failure for the antivirus industry and noted he and his colleagues may be “out of their leagues in their own game.” Though millions around the world rely on these tools, it’s pretty clear the antivirus era is over.

One of the reasons it is proving difficult to counter the wide variety of technological threats in our lives today is that there has been a burgeoning increase in the number of so-called zero-day attacks. A zero-day exploit takes advantage of a previously unknown vulnerability in a computer application that developers and security staff have not had time to address. Rather than proactively looking for these vulnerabilities themselves, antivirus software companies generally only consider known data points. They’ll block a malicious bit of code if it’s just like the other malicious bits of code they have seen previously. It’s essentially like putting up a wanted poster for Bonnie and Clyde because we know they have robbed banks previously. Bank tellers would know to be on the lookout for the couple, but as long as no one fitting that description materialized, they might let their guard down—until a different bank robber struck, that is. These zero days are increasingly being generated for a wide variety of techno-products commonly used in our lives, affecting everything from Microsoft Windows to Linksys routers to Adobe’s ubiquitous PDF Reader and Flash Player.

Eventually, hackers figured out that the more noise they made breaking into your systems, the more quickly you would fix the problem and kick them out. Now it’s all about stealth and clandestinity, like having a sleeper cell in your computer. You might think the abysmal 5 percent computer virus detection rate revealed in the Imperva study applied only to average citizens using personal security software in their homes. Surely businesses with their massive budgets for information technology and security would fare much better against hackers? Not so much. Tens of thousands of successful hacks against major corporations, NGOs, and governments

around the world reveal that enterprises, for all they spend, are not much better in protecting their own information.

According to Verizon's *2013 Data Breach Investigations Report*, most businesses have proven simply incapable of detecting when a hacker has breached their information systems. The landmark survey carried out by Verizon business services, working in conjunction with the U.S. Secret Service, the Dutch National Police, and the U.K. Police Central E-crimes Unit, reported that on average 62 percent of the intrusions against business took at least two months to detect. A similar study by Trustwave Holdings revealed that the average time from the initial breach of a company's network until discovery of the intrusion was an alarming 210 days. That's nearly seven months for an attacker—whether organized crime, the competition, or a foreign government—to creep around unfettered in a corporate network stealing secrets, gaining competitive intelligence, breaching financial systems, and pilfering customers' personally identifiable information, such as their credit card numbers.

When businesses do eventually notice that they have a digital spy in their midst and that their vital information systems have been compromised, an appalling 92 percent of the time it is not the company's chief information officer, security team, or system administrator who discovers the breach. Rather, law enforcement, an angry customer, or a contractor notifies the victim of the problem. If the world's biggest companies, firms that collectively spend millions on cyber defense and have whole departments of professionals working 24/7 to protect their networks, can be so readily penetrated by hackers, the prospects for home users protecting their information look grim indeed.

How hard is it to break into the average computer system? Laughably easy. According to the Verizon study, once hackers set their sights on your network, 75 percent of the time they can successfully penetrate your defenses within minutes. The same study notes that only 15 percent of the time does it take more than a few hours to breach a system. The implications of these findings are profound. From the time an attacker decides to target your world, 75 percent of the time the game is over in minutes. You'll be punched, knocked out, and on the floor before you ever knew what hit you. In today's world, hackers are living unfettered and

free inside your very own data systems for months and months, watching, waiting, lurking, and pillaging everything from your passwords to work projects to old selfies. You are easy marks and sitting ducks. How odd that we as a society tolerate this. If any of us noticed a burglar in our home watching over us as we slept or filming us in the shower, we would immediately dial 911 (or alternatively scream or reach for a gun). In cyberspace, this is a daily occurrence, yet most of us remain calmly, even blissfully unaware of the threat, despite our deep vulnerabilities and the bad guys looming over us as we sleep.

The cost of our universal cyber insecurity continues to mount. Though businesses around the world may be on track to spend nearly \$100 billion by 2017 for a variety of software and hardware security measures, that price is merely a starting point when considering the full economic impact of our technological fragility. Take, for example, the 2007 cyber strike against TJX, the parent company of the retail stores T.J. Maxx and Marshalls in the United States and T.K. Maxx throughout Europe.

In that case, hackers stole the credit card details of over forty-five million customers, making it the largest retail store hacking case of its time. Later in court filings, it was revealed the actual number of victims was closer to ninety-four million. Though TJX reached a settlement with Visa, MasterCard, and its customers in the amount of \$256 million, many analysts believe the true costs could easily have been closer to \$1 billion. One of the most authoritative sources for research on the cost of data breaches comes from the Ponemon Institute, which conducts independent research on data protection and information security policy. In calculating cyber-security breaches, it notes it is important to extend the loss analysis well beyond direct consumer theft amounts.

For example, the victim company targeted in the attacks, such as TJX, must spend handsomely on detecting the breach, containing the attackers, investigating the matter, identifying the perpetrators, and repairing and recovering its computer network. Moreover, there are often heavy sales declines as a wary public shies away from using the services of a company perceived to be unsafe and insecure. Add to that the price of credit card replacement fees (currently estimated to be \$5.10 per card), consumer

credit-monitoring services that need to be purchased by the victim company to prevent ongoing credit card fraud against its customers, and rising cyber-insurance premiums, and it is easy to see how quickly the costs of these losses can escalate. No wonder most companies are loath to admit that they have been hacked and many attempt to deny the breach as long as possible.

There are yet even greater costs to be considered, including how the stock market punishes victim firms via precipitous drops in their stock prices after a cyber intrusion. In one case, Global Payments saw its market valuation slashed by 9 percent in just one day until the New York Stock Exchange halted trading of its shares. Adding to the financial headaches in these cases are the ensuing class-action lawsuits from a firm's customers and shareholders, and from regulators. All told, the Ponemon Institute estimates that companies face nearly \$188 in costs for each and every record stolen. Multiply that amount by the nearly 100 million account records stolen at TJX, and it's easy to see how quickly the cost of these breaches escalates and grows exponentially.

All told, between the sums spent on mostly ineffective prevention measures and retroactively closing the cyber barn door after the horses are out (and the hackers are in), we pay dearly as a society for our technological insecurity. Worse, our growing connectedness to the networked world and our concomitant radical dependence on wholly penetrable technologies can bite in ways that hurt much more than our collective wallets.

The Internet has lost its innocence. Our interconnected world is becoming an increasingly more dangerous place, and the more we incorporate assailable technologies into our lives, the more vulnerable we become. The next Industrial Revolution, the information revolution, is well under way, with massive yet unrealized implications for our personal and global security. Yet as daunting as the threats to individuals, organizations, and even our critical infrastructures seem today, there is a proverbial technological train leaving the station, one that is rapidly and exponentially picking up speed. There are signs of it everywhere, if one knows where to look.

Just over the horizon are newly emerging technologies, including robotics, artificial intelligence, genetics, synthetic biology, nanotechnology, 3-D manufacturing, brain science, and virtual

reality, that will have major impacts on our world and pose a panoply of security threats that will make today's common cyber crime seem like child's play. These innovations will play essential roles in our daily lives in just a few years, yet no in-depth, broad-based study has been completed to help us understand the unintended attendant risks they pose.

The depth and extent of this transformation and its concomitant risks have gone unnoticed by most, yet before we know it, our global society will connect as many as one trillion new devices to the Internet—devices that will permeate every aspect of our lives. These persistent connections will bind us to both man and machine, across the planet, for good and for ill, and will be woven into the entire realm of our exponentially expanding common sentience. As a result, technology will no longer be just about machines; it will become the story of life itself. Those who know how these underlying technologies work will be increasingly well positioned to exploit them to their advantage and, as we have seen, to the detriment of the common man. The cornucopia of technology that we are accepting into our lives, with little or no self-reflection or thoughtful examination, may very well come back and bite us. These risks portend the new normal—a future for which we are wholly unprepared. This is a book about man and machine and how the slave may become master.