Article

Prepared by: Caroline Shaffer Wes
California National University for Advanced S

Engine of the Information Technology

MARK WILKINSON

Learning Outcomes

After reading this article, you will be able to:

- Address the fact that the majority of the world's data is unstructured.
- Identify the role of "big data analytics" in enabling businesses to analyze and extract value from data.

Data is pouring in from every conceivable direction: from inbound and outbound customer contact points, from mobile media and the web.

It is not just the volume of data—it is the unprecedented velocity and the variety of formats. The majority of the world's data is unstructured—whether it be text, images or video. Perhaps the simplest way of putting it is the amalgam of all this information is big data.

The result is that organizations now have untapped reserves of data which could deliver financial benefits to the emerging information economy. Most of the world's data has been created in the last few years and by 2020 the amount of information stored worldwide is expected to be 50 times larger than today.

This might at first appear to be a problem for businesses wanting to make sense of all this data. The reality is that data is the new oil that will power the information economy. But, just like oil, it needs to be put through the equivalent of a refinery to become valuable. This can be achieved through big data analytics, which enables organisations to analyse and extract value from all this crude data.

The insight derived gives them the power to know more about their business–not only the things they knew they didn't know, such as valuable customer information, but even the hidden gems that they had no idea even existed. Imagine being able to analyse data to determine the root cause of manufacturing failures or detect fraudulent behavior before it affects revenue?

Advances in computing power mean big data ana
deliver answers more quickly—what may have take
weeks can now be done in minutes or seconds. Che
storage and cloud-based services also make it accessib
organizations. Research by SAS and the Center for E
and Business Research, an independent consultancy,
that big data could deliver additional revenue of £21
the UK economy over a five-year period—equivalent
20 percent of UK net debt.

Only 14 percent of large companies have adopte
analytics, but this will more than double by 2017 ac
research by SAS and e-skills UK, the employer bo
digital industries. A major barrier to adoption is a s
skills. The same research predicts the number of bi
cialists demanded by business will grow by nearly 2
over the five years to 2017, yet three in five busines
struggle to hire people with these skills.

The government has highlighted the issue in bot
mation Economy Strategy paper and Strategy fo
Capability and acknowledged the need for busine
demia to work together with them to nurture the sk
Otherwise the UK risks losing out to other econor
the world. There is no time to waste in extracting
our new big data assets—the new oil that will driv
mation economy.

Critical Thinking

1. Is it reasonable to project that by 2020 the amount
information stored worldwide will be 50 times larg
is today? Explain.
2. How is it that our "new big data assets" can be cor
new oil that will drive the information economy"?

Create Central

www.mhhe.com/createcentral

Article

Prepared by: Caroline Shaffer Westerhof,
California National University for Advanced Studies

A Beginner's Guide to Building Botnets—with Little Assembly Required

For a few hundred dollars, you can get tools and 24/7 support for Internet crime.

SEAN GALLAGHER

Learning Outcomes

After reading this article, you will be able to:

- Recognize that an entire market of low-cost and easy-to-access software and services exists.
- Understand the scope and scale of cybercrime in terms of both the types of crime there are and the size of attack that is possible.

Have a plan to steal millions from banks and their customers but can't write a line of code? Want to get rich quick off advertising click fraud but "quick" doesn't include time to learn how to do it? No problem. Everything you need to start a life of cybercrime is just a few clicks (and many more dollars) away.

Building successful malware is an expensive business. It involves putting together teams of developers, coordinating an army of fraudsters to convert ill-gotten gains to hard currency without pointing a digital arrow right back to you. So the biggest names in financial botnets—Zeus, Carberp, Citadel, and SpyEye, to name a few—have all at one point or another decided to shift gears from fraud rings to crimeware vendors, selling their wares to whoever can afford them.

In the process, these big botnet platforms have created a whole ecosystem of software and services in an underground market catering to criminals without the skills to build it themselves. As a result, the tools and techniques used by last years' big professional bank fraud operations, such as the "Operation High Roller" botnet that netted over $70 million last summer, are available off-the-shelf on the Internet. They even come with full technical support to help you get up and running.

The customers of these services often plan more for the short term than the long game played by the big cyber-crime rings. They have very different goals. Botnet infrastructures can be applied in lots of ways for different sorts of profit—cash, information, or political gain. There are many ways to make money off botnets beyond outright theft, such as using them to steal advertising clicks, generate spam e-mails for a paying client, or renting out bots for denial-of-service attacks. And the same basic principles used to distribute botnets have been creeping up in more targeted attacks to steal intellectual property or to spread the malware used in the recent "wiper" attack on South Korean banks and broadcasters.

So how easy is it to get into the botnet business? Well, Ars decided to find out. Given the surprising availability of botnet building blocks online, I set out to build a shopping list to understand how everything is bought and sold within this black market. It all started with checking sources through a few Web searches then making trips into Web forums I dared visit only with a virtual machine and Google Translator's help. All I had to do was paste in "botnet" in Cyrillic, and I was on my way down the rabbit hole.

To assemble your list for some of the simplest get-rich-quick schemes, all you need is about $600, a little spare time, and no compunctions about breaking laws to make a profit. I didn't deploy an Ars-enal of botnet destruction in the end, but I absolutely could have. That may be the scariest lesson here.

It Looks Like You're Trying to Build a Botnet . . .

There are no personal shoppers to help walk you through the underground marketplaces to identify what fits a particular criminal scheme—though there may be plenty of people willing to give you paid advice on how to get started. With absolutely no budget for bitcoins, I got my start with some help from Max Goncharov, a security researcher for Trend Micro who specializes in following the Russian underground marketplaces for online fraud services. Goncharov came to Washington, DC in late March for a Trend Micro press briefing, and he laid out some of the basic things that go into a beginner fraudster's software and services shopping cart: botnets, malware-spreading tools, and hacking for hire. (Goncharov detailed some of these services in a paper published late last year and presented during this press road show.) Goncharov's suggested setup came with a $595 price tag for the first month of operations and a monthly cost of $225 to sustain the operation.

Of course, that price is for a particular type of botnet. It isn't representative of everything that's running wild on the Internet today. It also assumes total noob-hood. For those seeking to do something a little less overtly criminal than stealing credit card numbers or committing wire fraud, there are less expensive options. With a little sweat equity, you can pull off a workable botnet for a fraction of that price. If you're willing to try it without the benefits that come from paying professionals—like software updates, monitoring services, and 24/7 technical support—you can cut the cost back even further.

With my rough estimate in place, it was time to actually start some research of my own. Hello overseas VPN connection, Google Translator, and Google.ru—time for the underground hacker marketplace.

The Marketplace of (Bad) Ideas

The "underground" forums do more than just give would-be criminals access to a level of service that might make some enterprise software companies look bad. They also act as a sort of hiring hall for people with very specific skills (like hacking webmail accounts) or botnets of their own ready to do a paying customer's bidding. On these barely underground sites, hacker wares are made available to anyone willing to pay. Current versions of Zeus and SpyEye botnet software are for sale, or you can find the last version cracked by someone for cheap or free.

Many of the sites run under the thin veneer of "security" discussion boards. But they're often paid for by advertisements for the tools sought by a certain class of cyber-criminal: botnet-herders and the service provider ecosystem that has sprung up around them. These are largely the small and medium businesses of cybercrime, following a well-worn approach to making money. If you cast a big enough net, you're bound to catch some fish.

The botnet herders' standard business plan is to "use exploit kits, and then run a phishing campaign or some sort of campaign against massive numbers of people with hopes that someone is going to click on a link and get the exploit to drop a botnet or banking trojan onto their machine," said Nicholas J. Percoco, senior vice-president of Trustwave and head of the company's SpiderLabs penetration testing and security research team. "Once they've done that, it goes down the path of them monitoring them when they do banking transactions, or the botnet may be involved in spam or distributed denial of service attacks. Or maybe it's a sort of Swiss Army knife botnet that can do many different things depending on what that botnet herder decides, or what he makes it available to do for people who want to utilize his or her botnet."

No matter what the racket, Percoco told Ars, the equation for botnet herders is the same. "From a criminal's perspective, they're looking at massive numbers of attacks to achieve their financial goals."

They're also looking at massive turnover. When a piece of malware like a botnet lands on thousands of PCs, "it may hit the radar of an antivirus company pretty quickly," Percoco noted. That means time and money spent on finding new victims, deploying patches and updates, paying for new exploits, and generally continuing the game of "whack-a-mole" with antivirus companies and other organizations—as the mole.

Building a Botnet Shopping List

I did some additional research afterward to check Goncharov's math, and I also looked at some alternative approaches. The underground software market for hacking, fraud, and botnet tools has matured to the point where developers provide most of what you'd expect from legitimate software and online service providers—maybe even more. There's full support for the paid services, including 24/7 voice support in some cases, in a business where positive word of mouth in forums is the best (and often only) advertising. And there's no shortage of "consultants" to help you get started.

Botnet software itself is an important part of the whole equation, but it's only a fraction of first-month startup costs—and one that's fungible if you're willing to invest some of your own sweat equity in the setup (or dispense with the "legitimate" route and use a cracked version without software support). Just like any Internet business, launching a financial fraud botnet—or any kind of long-running botnet endeavor—requires a sustainable business plan. You need to know your target market, ensure distribution, keep your installed base a step ahead of the competition, and keep your business processes secure.

Here's a typical botnet-herder's startup shopping list:

A "Bulletproof" VPN

Before you start building a bot army of incredible magnitude, you need—just as with any other hacking endeavor of questionable legality—to hide yourself from prying eyes. That means using some sort of tool to avoid monitoring by your ISP, law enforcement, and other cybercriminals. Generally speaking, the best way is a virtual private network.

As confessed LulzSec member Cody Kretsinger found out, not all VPN providers are created equal. He used a service called HideMyAss.com, a VPN and proxy service run by UK-based Privax Ltd. Unfortunately, he didn't read the company's privacy and legal policies, and they gave up his logs when law enforcement came knocking. "Bulletproof" VPN services are ones that claim to be shielded from law enforcement requests because of their location or logging practices. Many of these services have disclaimers about "abuse" of the services, but the fact is that they take a number of anonymous forms of payment (CryptoVPN, for example, accepts Liberty Reserve, Bitcoin, and a number of other similar anonymous payment services). At worst, these services may just cancel your account if it attracts too much trouble.

A typical "bulletproof" VPN service, such as CryptoVPN runs about $25 a month. If you're thinking long-term, you can sign-up for $200 a year. However, it's best not to think long-term if you're botnet-herding; it may behoove you to change services every now and then to keep your profile low.

Budget Botnet Shopper's Price: $25/month.

A "Bulletproof" Host

Once you've got your network secured, you need some place to host your botnet's command and control network and all of the other assorted badness needed to launch a massive assault on the unsuspecting world. For those without the skills, time, or desire to simply go hack someone else's server every couple of weeks, that means buying a dedicated or virtual dedicated server from someone who doesn't care what you're doing—lest your botnet's nerve center be wiped during a security sweep or seized by law enforcement.

There are many kinds of "bulletproof" hosts catering to various kinds of customers. Most of them buy space in data centers around the world in places with either weak data privacy laws or plain disregard for what other countries' laws say. This provides a sort of insurance policy for their customers, Goncharov said. At a minimum, the data on the servers won't be given up to law enforcement.

Some are smaller hosting companies such as Hostim VSE, a Romanian hosting company with a Russian language website more targeted at protecting pornographers, pirates, and other targets of DMCA takedown requests. Hostim VSE publicly denounces botnetters and financial fraudsters to prevent tion from local law enforcement. It describes "bulle hosting" as "hosting resistant to complaints and other of attacks on competitors. When placed on a standard w hosting, your site can receive complaints from compe under the guise of copyright holders. In consequence o most other hosting providers disable your site until the ci stances [change]. We also review all such complaints, che validity, conduct a site audit, demand [the accuser] to pr documents confirming the rights, and otherwise deal with settle the conflict, and only then disable the client's site."

All of this, the company says with a wink, takes a lot o and human resources, and as a small company there m some delays before it gets around to it. In other words, " worry—we're inefficient." Hostim VSE's dedicated se start at $39/month with additional charges for more bandv The company also, ironically, provides DDoS protectio other support services. But prices for its services will rise matically if you're attracting too much attention or usin much bandwidth.

For really hard-core criminal undertakings, there ar more specialized underground "bulletproof" hosting ser that are run specifically for malware owners. These offer ing at a significant markup in exchange for looking the way. These operations generally don't maintain webp They advertise strictly in underground forums and do bus over ICQ, Jabber, and other instant messaging.

Mihai Ionut Paunescu, the 28-year old Romanian be underground host powerhost.ro, was caught in Decembe Romanian authorities. His servers were home to the Gozi f cial malware command and control network. Paunescu tabs on exactly what sort of business his users were up to charged accordingly. In some cases, the rates reached sands per month, averaging better than a 100-percent marg the servers he managed.

Of course, many of these hosting companies provide sup (in some cases, 24-hour voice support via phone or Skype) help with configuring Apache and MySQL on dedicated for customers who are generally clueless about such things

Budget Botnet Shopper's Price: $50/month, plus "consulting."

Bulletproof Domains and "Fast Flux"

In order for your bots to reach your host reliably, you some domain names—fully qualified domain names that a you to have full control over the domain name service (D You'll want a bunch so you can avoid making yourself obv in the DNS logs of networks that get infected.

You'll also want to register those domains with a registrar that's not going to roll on you and shut you down on the first complaint of abuse. You need someone who will shield your identity from the prying eyes of security firms and law enforcement. In other words, you want a bulletproof registrar. Preferably, it's one that accepts payments via Western Union or some other anonymous service.

Of course, it's never a bad idea to have some additional protection to make sure that you cover your trail completely by using a "fast flux" scheme. This hides your servers' true location by assigning the DNS addresses to a rapidly changing set of proxies. Fast flux providers will take your domains—or even register them for you—and then assign host names to a collection of their own bots. These in turn pass traffic between your bots and your server. By using a short "time to live" for the host "A" name records in the DNS server, fast flux systems create hundreds of potential communication paths for the bots.

Fast flux service is costly. An advertisement on one forum recently offered to support five DNS name servers for customers starting at $800. So for most starting botnet operations getting their feet wet, just registering a few domain names may be enough to begin with.

Budget Botnet Shopper's Price: $50 for five domains.

Your Choice of Botnet/C&C Platform

The current editions of botnet-building frameworks are sometimes sold by their developers for premium prices. Carberp was sold by its developers prior to their recent arrest for a whopping $40,000 as a kit, while the current Zeus toolkit sold for about $400 when it first hit the market. But the market pays what the market can bear, and most first-timers can find less expensive options that are easier to sustain.

Do-it-yourselfers who don't care about things like patches and full support can find "cracked" versions of some of these toolkits (or ways to disable their licensing code) for free. There's also an option to pick up older but still supported versions on the aftermarket. Zeus' source code was released to the world last year, sort of turning it into "open source," so you can now purchase supported versions of it for $125, plus $15 per month for updates to the code and $25 for monthly 24/7 new customer support. That could include everything from helping a noob fix a misconfigured server to doing a whole walkthrough of configuring the PHP scripts and MySQL backends for the system over Skype. You could always just use one of those YouTube guides, though, and save some money.

Budget Botnet Shopper's Price: $125, plus $40/month for support.

Web Attack "Injector" Kits

The Zeus botnet's market dominance has created a whole additional ecosystem of software add-ons to make its bots do various things. A big part of that market is "injectors"—the add-on modules that tell the bot what to watch for in browser activity and what code to inject into the browser when it visits targeted websites.

There are financial botnet injectors that insert Web code into banking sites. These injectors try to grab your personal information to hijack your account, make wire transfer withdrawals, or even change the values presented in your online statement to conceal all of it.

Other types of injectors could be used for things like click-fraud—changing the links that users click on to direct them to different websites, while sending a referral code to a Web advertising provider to collect the pay-per-click. Some new botnets have been configured to simply generate clicks in the background on webpages without the computer user seeing them, creating ad revenue without the user scratching his head about why he ended up on a Russian porn site instead of the car insurance site he was trying to visit.

Beginners can buy injector packs for a set of banks through marketplaces and pay for direct support to help install, tune and customize them. In some cases, these require some server setup as well to properly harvest the data collected. It sounds complicated, but there are people happy to help you figure it all out for a small fee.

Budget Botnet Shopper's Price: $80, plus $8/month for support.

An Exploit Tool or Service

In order to take command of victims' PCs, a bot herder needs a reliable way of defeating the basic security provided by operating systems, browsers, and e-mail anti-virus scanners. That usually means relying on an "exploit pack" or some other crafted application exploit.

The modus operandi of most bot herders is to use Web links as the delivery method for their malware, sending out streams of spam to potential victims in the hope that someone will fall for their social engineering. One click leads to a webpage set up to drop a package of nastiness on them. There are ready-made exploit packs, loaded with code written specifically for the purpose of planting malware on victim's PCs that can be purchased and installed on a Web server or "rented" as a service.

Botnet builders can rent capacity on these services or outright buy them. A Phoenix exploit kit (like the one used to seed the recent Bamital botnet), can be purchased for $120, plus another $38 per month for patches and technical support, according to Goncharov. BlackHole, another market leader in

exploits, offers its latest and greatest as a leased service for $50 a day, with extra fees for traffic overages. BlackHole also comes with an Oracle-like annual license for those who want to deploy on their own server. That costs $1,500 per year, with various add-on functionality fees.

Budget Botnet Shopper's Price: $120 for the kit, plus $38/month for support.

Crypters and Dropper Builders

The problem with just pushing a Zeus bot in its raw form out to targets through an exploit is that the Zeus bot is bound to be detected by antivirus software because of its signature. To prevent that, botnet-herders turn to "dropper" malware that disguises the bot trojan, delivering it in encrypted form to disguise the file signature of the trojan and its associated files.

Creating a "dropper" requires the services of a malware "crypter." Some are sold as straight software, with added services to see if the signatures of built droppers have been picked up by antivirus companies' databases. Others are sold purely as a service, with timer-based licenses, and may include the antivirus signature check as a built-in service.

There are even crypter services now available on the Web, delivered as a service. One such service offers dropper-building at the rate of $7 per "sample."

Another key to not getting caught is "antisandbox" code that detects if the malware has been dropped onto a sandboxed system or virtual machine—such as those used by digital forensics experts and security analysts. If the code detects that it's been deposited inside such a system, it can prevent the botnet trojan from being deployed and giving up the nature of the code it carries. Antisandbox code is a feature of some crypters.

If you want to save some money—and aren't particularly concerned about whether your bot gets picked up after a while by antivirus scans—there are sites offering "cracked" crypter kits for free.

Budget Botnet Shopper's Price: $20/month for crypter and accessory licenses.

Special Delivery: Spam and Social Engineering Services

But wait! You still have to deliver the exploit link to drop your botnet package on your unsuspecting (or possibly suspecting) victims. How do you get them to click on that link? The traditional route is by blasting semi-convincing spam messages and hoping people are dumb enough to click on a link in them to see a video, download a document, or reconfirm their PayPal information.

That typically means buying a spam blast, often from a botnet operator. Some spam-masters have moved their f social networks and charge not per message but per hit. Y spam out to social networks and over SMS with clickjac using "borrowed" credentials or leave it to the professio do it for you for around a buck per thousand targets.

But that's the old-fashioned way. The new-fashioned to use "spear-phish" attacks that use social informatio the target in some way that convinces them to click t either through a social network message in a compr account or an e-mail that appears to be from a friend. want to make it even more convincing, you can alwa someone to hack a victim's e-mail address to get access account and contacts. Then it's as simple as posing as tim to fool all their friends.

For beginners, spam remains the best bet. It can be hit a variety of potential targets and it's relatively cheap spamming services can run as little as $10 per 1 millio addresses, with better services based on stolen custom bases running five to ten times as much.

Budget Botnet Shopper's Price: $50 for an initial qualified addresses.

Economies of Scale

Using our budget shopper prices, that adds up to about $ the first month of operation.

None of these purchases guarantee success, obviou it could take multiple spam attempts and help from ot cialists to finally establish that botnet you've dreamed then, the payoffs are not necessarily that big. There's botnets already out there and botnet herders may be up a short window before detection.

On the upside, it's an easy game to buy into—unlike ger, more enterprise-scale cyber-crime rings behind bi rate data breaches. While the whales of the cybercrim may share some of the basic technology approaches w smaller cousins, they have more in common with t lectual property stealing "Advanced Persistent Threat hackers alleged to be associated with the Chinese (though they may surpass them in skill). Trend Mic Technology Officer Raimund Genes said during the D ing that he thought the recent alleged Chinese APT had been uncovered largely because they lacked the fi Eastern European cybercrime rings.

The bigger financial hacking organizations—whi small number of organizations of hundreds or perha thousands of people—operate in their own closed sometimes on "darknets," where you can only gain a being invited. While there's some use of botnets by t

cyber-crime rings, they tend to want to protect their investments in the more specialized, targeted attack tools they use. Botnet use is sparse in that space. "Once they get access to the environment," Percoco said, "they then deploy custom pieces of malware that are sometimes written from scratch, brand new, never been utilized before—and they plant them on specific systems within the environment."

As a result, the data breaches caused by these targeted hacks can go on for months, even years before being detected. A study released by Percoco's team at Trustwave in February found that the average targeted attack went more than 210 days before it was detected. And this detection was usually because of a customer complaint or notification by law enforcement or a payment processor, not because antivirus software detected the hack. At some companies, the hacks lasted more than three years without being detected, all while millions of credit card transactions and other data were being pumped back to the hackers.

Botnet operators generally go big or go home in their attacks. But the tools they use can just as easily be applied to the long game if they're used in a targeted fashion and they apply some of the lessons learned by the big-time hacking organizations. "Swiss Army knife" botnets and remote administration tools can be used as part of a poor man's APT by those who are willing to take the time to do the research and social engineering to get their malware in the right place. And just because Zeus and other botnets are a known threat doesn't mean they can't be used in stealth. According to the site ZeusTracker, the average detection rate for Zeus binaries by antivirus software is only 38 percent. And that's for **known** Zeus botnets.

So take heart, would-be botnetter. With the market saturated with tools, a community of several thousand known botnet operators, and new ways to profit emerging every day, your first botnet could bear a return on investment hundreds of times larger than what you put in. You don't need to know the first thing about coding. Though a lack of morality wouldn't hurt either.

Critical Thinking

1. Given the editors of this reader (or of Ars Technica) are not training hackers, why do you think this article was written and why does it appear in this reader? What are the principal lessons a non-hacker should take away from this article?
2. If there is a known online marketplace for cybercrime software and services, why do you think it is that the authorities simply don't shut it down?

Create Central

www.mhhe.com/createcentral

Internet References

The Geeks at the Frontlines
www.rollingstone.com/feature/the-geeks-on-the-frontlines#i.14f11oq1e28f09

James Lyne: Everyday Cybercrime—and What You Can Do about It [TED Talk]
www.ted.com/talks/james_lyne_everyday_cybercrime_and_what_you_can_do_about_it.html

Rise of Domestic Drones Draws Questions about Privacy, Limiting Use
www.pbs.org/newshour/bb/science/jan-june13/drones_04-18.html

Shodan: The Scariest Search Engine on the Internet
http://money.cnn.com/2013/04/08/technology/security/shodan/index.html?iid=EL

Article

Prepared by: Caroline Shaffer W
California National University for Advanced

Network Insecurity

Are We Losing the Battle against Cyber Crime?

JOHN SEABROOK

Learning Outcomes

After reading this article, you will be able to:

- Understand what cybercrime is, as differentiated from traditional crime.
- Understand what cybercrime is, as differentiated from hacktivism, and cyber espionage.
- Be familiar with specific terminology of cybercrime used by Seabrook including: botnet, DDoS, phishing, spear phishing, key logger, malware, and rootkit.

Richard McFeely, of the F.B.I., is a former insurance adjuster from Unionville, in eastern Pennsylvania horse country. He has a friendly face, meaty hands, and a folksy speaking style that doesn't seem very F.B.I.-like. "Call me Rick," he said, when I met him at his office, in Washington, coming around his wide desk and gesturing toward the soft furniture in the front part of the room.

McFeely, who is fifty-one, and whose official title is executive assistant director ("E.A.D.," in office shorthand), oversees about sixty per cent of F.B.I. operations, including the Cyber Division: some one thousand agents, analysts, forensic specialists, and computer scientists. The bureau has made several high-profile takedowns in recent years, including the dismantling of the Coreflood botnet, a network of millions of infected "zombie" computers, or bots, controlled by a Russian hacking crew.

"But we are just touching the tip of the surface in terms of what companies and what government agencies are at the most risk," McFeely said, shaking his big head ruefully. "We simply don't have the resources to monitor the mammoth quantity of intrusions that are going on out there." Shawn Henry, McFeely's predecessor at the F.B.I., told me, "When I started in my career, in the late eighties, if there was a bank robbery, the pool of suspects was limited to the people who were in the vicinity at the time. Now when a bank is robbed suspects is limited to the number of people in the access to a five-hundred-dollar laptop and an Inter tion. Which today is two and a half billion people." of stealing just one person's credit card, you can millions of people at the same time. This may hav when, in 2011, PlayStation's gaming network was its members' credit-card data compromised.

"It's not the eighties," Tony Stark sneers, in "Iron M one says 'hack' anymore." Hacking used to mean hip ogists who wanted to set information free. Now hac organized criminal gangs, working out of the former who steal financial information; or state-affiliated spi who are carting away virtual truckloads of intellectu or saboteurs in Iran or in North Korea who are tryin or destroy critical infrastructure—not to mention al scale criminals downloading hacking tools and launc because this shit is cool and you can't get caught.

General Keith Alexander, who is the head of the of the U.S. Cyber Command, has called the loss o industrial secrets and intellectual property to cybe "the greatest transfer of wealth in history." Plans f jet fighter, source code from Google, and details a Cola's 2009 bid to buy China Huiyuan Juice Grou stolen. The *Times* and the *Wall Street Journal* both January that Chinese hackers penetrated their ne year, apparently in order to gather intelligence abou stories on Chinese officials. Until recently, the U. reluctant to publicly accuse China of spying, but Tom Donilon, President Obama's national-secur spoke of "cyber intrusions emanating from China on edented scale." This month, the Pentagon released a bluntly accused the Chinese military of cyber espio denies these accusations.

China is by no means our only cyber-securit Organized criminal gangs, loosely affiliated with n

constitute an entirely new category of threat. As the world moves online, traditional boundaries break down, and whether it will ever be possible to secure the Internet is an open question. McFeely, his voice rising plaintively, said, "The cyber bad guys have evened the playing field! In the past, we knew it was the traditional big players who were spying on us. Now you get these small countries that are trying to gain a competitive advantage in some industry. So they can go and hire a hacking group, specifically target a company, and steal years and years of R. & D."

In October, Leon Panetta, the Defense Secretary at the time, warned that "an aggressor nation or extremist group could gain control of critical switches and derail passenger trains, or trains loaded with lethal chemicals," resulting in a "cyber Pearl Harbor." Privacy advocates criticized the statement as scaremongering, suspecting that Panetta's ulterior motive was to increase government oversight of the Internet. Approximately eighty-five per cent of the critical infrastructure in the U.S. is privately held, and the government's authority over it is limited. The Cyber Security Act of 2012, which would have asked companies to comply with basic security regulations, died in the Senate last year. Republicans thought that the regulations would be too expensive and would entail too much government oversight.

The Department of Homeland Security reported a hundred and ninety-eight attacks on critical U.S. infrastructure in fiscal year 2012; there were just nine attacks in 2009. These included the penetration of twenty-three oil and natural-gas pipeline operators and six attacks on nuclear power plants. Last year, hackers also broke into an unclassified network in the White House Military Office. In all these cases, the intruders seemed more interested in snooping than in sabotage, though they could return, with more sinister intentions.

A large part of the nation's financial infrastructure is also under siege. The most furious wave of assaults began in September, when almost fifty major U.S. banks suffered "distributed denial of service" (DDoS) attacks, in which botnets—which can be controlled from afar with remote-access tools, known as RATs—directed high volumes of traffic to the banks' Web sites, causing them to run slowly or to crash altogether.

In many cases, the F.B.I. knows where cyber attacks originate, and in some cases it knows who the attackers are. Much of this information is gathered by the National Cyber Investigative Joint Task Force, an interagency group, based in an undisclosed location near Washington. But, even when hackers are identified, law enforcement is often powerless to confront them. "If you look at the typical attacks on a bank," McFeely said, "most of the attacks aren't coming from within the U.S. What's the stomach of our policymakers here to conduct a unilateral operation on foreign soil?

"I get sick to my stomach when I see that stuff," McFeely went on. "We literally watch our intellectual property leave the country. But, if we do stop it, we lose sight of the rest of it." The bureau would end up revealing its sources and methods to the enemy, while the hackers would simply move on to another target. "So it's a huge conundrum for us. Could the U.S. government do something about these attacks that the financial sector has been undergoing for over a year? Of course we could. The question is, what are the triggers that are going to cause us to take action and what will the impact be?"

From the earliest days of the Internet, the basic approach to network security has been to play defense. The idea is to secure the perimeter of a network with firewalls and intrusion-prevention systems that keep "blacklists" of suspect bits of code, and rely on algorithms which detect suspicious patterns; the algorithms are constantly updated as new threats emerge. Tom Kellermann, a vice-president of Trend Micro, a cybersecurity firm based in Cupertino, California, calls this approach "the citadel paradigm." It depends heavily on antivirus software and users' diligent updating of it. "You keep the crown jewels on the inside, and you build electronic walls and a moat around them," he told me. "It's like the Federal Reserve in lower Manhattan, where the gold is kept." This type of strategy works well when the attacks are opportunistic and random: the intruders are simply searching for an easy way in.

In recent years, however, the citadel paradigm has been battered by so-called "targeted attacks," in which the adversary goes after a particular government agency, company, or individual, with a specific goal in mind. This kind of determined adversary often uses a relatively sophisticated e-mail scam known as "spear phishing." Earlier phishing attacks tended to be clunky and scattershot, like the bogus-looking e-mails purportedly from Google asking you to verify your log-on information, or Nigerian banking scams, or the "Help, I've been robbed in Dublin, can you wire money to Western Union" e-mails supposedly from a friend but actually from a con artist who has hacked your friend's e-mail account. The flimflam was easy to sniff out, generally because the spelling was atrocious (bad guys apparently don't use spell-checkers). Toying with these hapless thieves—"I have wired a thousand dollars to the local police station, you can collect your reward there"—used to be good sport.

But a spear-phishing e-mail is tailored especially for you. Not long ago, the National Association of Manufacturers received an e-mail purportedly from a reporter at Bloomberg who was working on a story about the group, with an Excel spreadsheet contained in an enclosure. In fact, Chinese hackers had spoofed the reporter's e-mail address, and the enclosure contained espionage-related "malware": malicious code. Social networks make it much easier for hackers to impersonate friends and colleagues. "Here are the numbers we spoke about at last night's party"—the one you posted pictures of on Facebook. Downloading the attachment silently installs the malware, without your noticing; later, you may wonder why your computer's fan is always on (it's because the hacker is using your machine's extra computing power). Now you've

got a RAT in your machine, which can capture your passwords, credit-card numbers, and banking information, and can turn on your computer's microphone and camera. (Around this magazine's offices, people have started putting Post-it notes over their Mac's little Cyclops-eyed camera.) Your machine is now part of a botnet (in China, bots are called "meaty chickens"), and can be used to launch denial-of-service attacks or send out spam.

RATs also work on smartphones, turning them into ideal spying and tracking devices; you bug yourself, basically. No one is safe. A computer (and therefore any network) can be infected if you simply open an e-mail or visit the wrong Web site. And anyone can be hacked. Even RSA, the maker of the SecurID tokens that are supposed to keep intruders off networks, got hacked when an employee clicked on an enclosure in a spear-phishing e-mail with the subject line "2011 Recruitment Plan," ostensibly from beyond.com, a career-advancement Web site, and inadvertently installed malware on his computer. The hackers then captured passwords from that computer and used them to gain access to other machines on the network and steal some of RSA's data, which, in turn, allowed them to hack RSA's clients using duplicates of the now compromised security tokens. RSA subsequently offered to replace or monitor all of its tokens, which, as of 2009, numbered forty million. The same spear-phishing attack affected more than seven hundred and fifty other companies, including about a fifth of the Fortune 100. Dmitri Alperovitch, the co-founder and chief technology officer of CrowdStrike, a private security firm, summed all this up for me by saying, "The idea that any company in the world is going to be able to protect itself against an intelligence service or an armed military unit of another country is, quite frankly, ridiculous."

There are simply too many ways for an attacker to get into your computer now. If you log on to the office network with a smartphone, or if you carry a laptop between work and home (a workplace trend known as B.Y.O.D., for "bring your own device," although I heard security people say that it means "bring your own disaster"), you make it very easy for intruders to enter the office network. "In fact, some of the biggest espionage cases we're working on right now involve the home-to-work commuting thing," McFeely told me. "The company can have great security within its own walls, but as soon as it transits out you're at the mercy of the weakest link in the chain." With Wi-Fi hot spots, which can be easy to tap into, popping up everywhere, and with ever more network-enabled devices entering both the office and the home—smart TVs, smart front-door locks—intruders have a panoply of ways to break into your life. Several years ago, Best Buy was discovered to be selling digital picture frames that had been infected with malware.

"Up until four years ago, we kind of had a handle on this shit," Tom Kellermann says. "Virus scanning and encryption and firewalls were doing a pretty good job. But the latest attack kits are bypassing those perimeter defenses, which is wh paradigm has to shift."

I spent a day inside the citadel, with Google's security at the company's headquarters, in Mountain View, Calif As part of its mission to organize the world's inform Google tries to provide its users with a secure way to it. Google doesn't guarantee that it will protect its cust from cyber criminals and spies, but it has devised a num ways of alerting users to suspicious patterns that its s algorithms pick up. The company has been unusually coming about attacks. In January, 2010, for example, announced that it had fallen victim to an attack that c be known as Operation Aurora. (At least twenty othe panies, including Adobe, Intel, and Yahoo, were hit, Google was the first to make the information public.) quent analysis by cyber-security experts suggested that affiliated with the Chinese government were behind th and that they had exploited a vulnerability in Internet E to get onto Google's network and steal some of its sour Google's chief legal officer, David Drummond, wrote have evidence to suggest that a primary goal of the was accessing the Gmail accounts of Chinese hum activists." Although only two Gmail accounts were mised in the attack, Drummond said that the ensuing i tion revealed that the accounts of dozens of Gmail us U.S., China, and Europe who are advocates of hum in China appeared to have been routinely accessed parties.

Sergey Brin, one of Google's co-founders, told n invests a lot of time in keeping his security team "Corporate security teams are often low in morale," h October, at a conference in Arizona. (Brin, dressed cycling duds, was sporting Google Glass, Google's eyewear; sometimes I couldn't tell whether he was me or to the screen inside the lens.) He continued, " porations, people don't understand what security pec the most part, and no one pays attention to them un thing goes wrong. Frankly, a lot of companies aren' ested in security. They say they care, but they really are vulnerable, they can't do that much about it, and it. They're just waiting for something big to hap meets with the security team every Friday, to review catalogue of threats. Because Google and its users thousands of times each day, there is usually much

The team at Google is led by Eric Grosse, a so neer who came from Bell Labs, and includes Linus oversees security for Google's browser, Chrome; who handles Web spam; Niels Provos, who leads G malware efforts; and Shane Huntley, who works threats, which include state-sponsored espionage paradigm works better in some of these areas th Google's anti-spam efforts are the brightest spot

landscape; spam is exactly the sort of mass, opportunistic attack that the defensive strategy was designed for. Web spam, which clogged up search-engine results, and unsolicited e-mails advertising prescription drugs, penis-enlargement methods, and casinos, which threatened to sink the Internet in the early two-thousands, have been all but eliminated by Google's anti-spam algorithms. "We like to say the spammers have the numbers, we have the math," Cutts told me.

Grosse and I discussed passwords, often the weakest link in the security chain. The recent takeover of the Associated Press's Twitter account by Syrian hackers, which caused a momentary hundred-and-fifty-point drop in the Dow, is an example of the kind of havoc a stolen password can bring about. "My goal is to get rid of passwords completely," Grosse said. "Perhaps you will still have a password but it wouldn't be a prime line of defense." In the short term, however, more passwords, not fewer, seems to be the solution. "We rolled out this two-step verification"—using two passwords, essentially. "The biggest problem is people can't be expected to remember two hundred passwords. I mean, I have two hundred passwords, and they're all different and they're all strong."

"How do you remember them?" I asked.

"I have to write them down."

"But then that piece of paper could be stolen."

"Yeah, but if your adversary is somebody on the other side of the ocean he can't get the piece of paper you have in a safe at home. If you're trying to guard against your roommate, then you need a new roommate." With the two-step process, you register your mobile number, and when you enter your first password, Google texts a unique code to your phone, and then you enter that.

For Upson, who works on securing Chrome, the principal threat is what's known as a "zero-day exploit": a kind of vulnerability, either in an operating system or in an application such as Flash, Quicktime, or Chrome itself, through which intruders can sneak into a computer. (Because the exploit is either unknown to the software vender, or has not yet been patched, it is said to have zero days of remediation.) Exploits can sell for hundreds of thousands of dollars on the black market. Upson told me that Chrome updates itself automatically to fix known exploits, rather than requiring the user to do it. But if an adversary does find his way into your machine through an unpatched hole, he said, "you are better off just throwing your computer away and starting again with a new one, because there are so many places for the malware to hide." That's especially true if the hacker uses a "rootkit," a type of malicious software that can conceal itself from the antivirus software that is supposed to detect it, making cleaning your machine extremely difficult.

One of the Eastern European crews' favorite ploys, Provos told me, is to masquerade as an anti-malware company. "You go to your computer and your screen flashes and you get this dialogue box that says, 'We found all this malware on your computer and you are really in deep trouble, but don't despair, if you pay forty dollars right now you can download this security solution.' So now the malware authors have got forty dollars and they also have complete control of your computer." The latest wrinkle in this style of attack is "ransomware"—a program that encrypts your hard drive and sends you a message that appears to come, for example, from the F.B.I.'s Cyber Division, saying that it has detected child pornography or pirated software on your computer and instructing you where to send money, in order to unencrypt your data.

State-sponsored political espionage is perhaps the most difficult challenge the Google team faces. Chinese targets include the so-called "five poisons": the Falun Gong, Taiwan, the democracy movement, and Uighur and Tibetan separatists; even the Dalai Lama's computers were hacked. But China isn't alone in practicing cyber espionage. Oppressive regimes from Syria to Bahrain use the latest cyber-surveillance tools, many of them made by Western companies, to spy on dissidents. Finfisher spyware, for example, made by Gamma International, a U.K.-based firm, can be used to monitor Wi-Fi networks from a hotel lobby, hack cell phones and P.C.s, intercept Skype conversations, capture passwords, and activate cameras and microphones. Egyptian dissidents who raided the office of Hosni Mubarak's secret police after his overthrow found a proposal from Gamma offering the state Finfisher hardware, software, and training for about four hundred thousand dollars.

Shane Huntley told me, "Our analysis shows that if you are engaged in democracy movements or talking about human rights there is a much greater than fifty-per-cent chance that you are going to be the subject of a targeted attack." He added, "We found that a range of high-level U.S. officials were also having their accounts hijacked" by spear-phishing schemes. "The breadth and depth is kind of amazing."

"It's clear now that relying on traditional tools like antivirus alone is not sufficient for defense," Eric Grosse said. Today, he said, the various social-engineering attacks, like spear phishing, "are actually quite good at tricking and ensnaring victims." To counter these threats, he went on, "dynamic defenses that evolve almost instantaneously" are required. "For example, attackers who use compromised Web sites to deliver phishing pages now often have to shift the location of their sites within a matter of minutes to avoid being caught by software that blocks them."

Adam Meyers, who is the head of intelligence for CrowdStrike, the security firm, walked me through a hypothetical corporate-espionage attack coming from China. Meyers, who is tall, techy, and wears four small earrings in his left ear (three in the lobe and one higher up, in the cartilage), began by noting that many patterns of corporate espionage bear a suspicious resemblance to China's five-year plans for modernizing the country's infrastructure. The scenario he conjured up involved

China's South Sea Fleet, one of three fleets that make up the naval branch of the People's Liberation Army, or P.L.A. The Chinese navy is known to be interested in expanding its capabilities from green-water activities—near to shore—and building up a blue-water, or deep-sea, presence. To do that, it needs to advance its satellite communications, boat building, robotics, and other technologies.

"So the P.L.A. naval officer says to his intelligence forces, 'Here's the five-year plan,'" Meyers said. "He's not using the military's élite hacking crews, because he doesn't want this traced back to the military. But there are plenty of crews for hire that are only loosely affiliated with the government, so he uses one of those. He says, 'Get me everything you can on these technologies.' So they go out and start their operation.

"The first thing they need to do is get access. That starts with open-source intelligence collection—same way you'd start a story, I imagine. They find out who the key people are at the tech companies they're interested in, and do a Google search. They get people, facilities, potentially who the company's software vendors are, and what kind of security software they run. They get the jargon they can use to start crafting an attack. And if they can't get access to you they will find out who your partners are and get access to them. It's all about exploiting a trust relationship.

"Then they run all the names through social media—Facebook, Twitter, LinkedIn—and map your personal relationships." The spear-phishing e-mail "could be a weaponized press release," Meyers continued. "If it's *The New Yorker* I'm after, I send your P.R. people an e-mail saying, 'Hey, we've got evidence your reporters are paying people for stories, we're going to go to press with this in the next twelve hours'—and attach the link. Chances are you are going to click on it." Attacks follow marketing guidelines on what day and time is best to send out e-mails that people will open. "Like Tuesday, late morning. Or they'll send something on a Friday, before a three-day weekend, because they know all the Americans are going away. Memorial Day is a big one. Then they've got until Tuesday before anyone even thinks of doing work"—giving them plenty of time to nose around the network.

Meyers showed me an e-mail that one of CrowdStrike's customers had received from a Chinese hacking crew, with the identifying information redacted:

> Dear Sir, I am writing to you to ask you for some information about [BLANK]. Our company plan to purchase five sets of [BLANK]. We are now ask for quote on this product. . . . Looking for your reply.

Below was an attachment with the header "Details About Requirement."

Not particularly convincing, I said, noting the poor grammar.

"Yeah," Meyers replied, "but if you're a sales guy and you see this come in the middle of the first week of the first quarter, and the guy plans to purchase five, and this is a n lar product—that's a five-million-dollar deal. So y up, it triggers a bug, and your Adobe Reader crash adversary controls the flow of that crash. As it goe installs the malware. So now they're in. They estab door and then start looking at your system to see wha are running."

In targeted attacks, the intruders generally know ex they are looking for, and can use your search tools around not just your computer but the office networ to move around, because most networks are built li "crunchy on the outside, but soft and chewy in th Meyers said, meaning that the networks lack stro security. "They install a key logger, dump your pass on the microphone, turn on the camera. Then they p different type of malware, so while the security guy fiving and having a cup of coffee, the second malwa lished and the hackers are still in. And, worse, we t stopped the problem. Then they push down tools them to move laterally across the network. Wher what they're looking for, they'll compress it, and enc exfiltrate it. And they'll leave a back door behind to they can come back in the future."

If the old paradigm was the citadel, the new para Kellermann, of Trend Micro, contends, is the pris not trying to build the Federal Reserve, you're tryi Rikers Island. Instead of trying to keep the bad gu keep them in, or you let them in the basement wher your Rottweilers, and you make life miserable for they are in, so they won't want to come back."

What would a cyber prison look like? To get a b spoke with Shawn Henry. With his shaved head and lis tough-guy demeanor, Henry is the G-man from c ing. Having retired as the E.A.D. overseeing the F.I Division last year, he is now a senior executive at C (where he continues to work with the former dep the Cyber Division, Steven Chabinsky, whom he br company). Part of his job is to impress clients with and the scope of their cyber-security problem. His ing eyes squint into a grim future as he conjures up cy and our lack of readiness for them. "When the electr alent of planes crashing into buildings occurs," he the lights go out, I guarantee you the public will be

CrowdStrike, which has an office in Crystal Ci is one of a new generation of security companies, s Eye, Damballa, and Mandiant, that offer clients active strategies—security and intelligence-gatherir bring the fight to the attacker in your system. "The mance measure was, Can you keep a determined a your network," Henry told me. "The new measure needs to be, How soon after they get access can yo so you can take immediate action."

In one instance, which Dmitri Alperovitch, of CrowdStrike, cited approvingly to me, the government of Georgia lured a Russian hacker, who had been breaking into government ministries and banks for more than a year, to a machine that planted spyware on the hacker's computer and used his Webcam to take his picture; the photographs were published in a government report. "The private sector needs to be empowered to take that kind of action," Alperovitch said.

But that kind of action, which is generally referred to as "hacking back," is illegal in the U.S. The same broad-reaching laws, grouped under the 1984 federal Computer Fraud and Abuse Act, or C.F.A.A., that the government uses to go after people like Aaron Swartz—the twenty-six-year-old activist who downloaded millions of articles from the JSTOR database—also limit private companies' powers to take offensive action. However, the C.F.A.A. is notoriously vague and out of date. "There are gray areas," Alperovitch told me. "What if the hackers stole malware that you had planted inside your network, and infected themselves? Is that illegal?"

Could those same gray areas allow the government to hack you? During Henry's time at the F.B.I., the agency developed malware and spyware for possible use in criminal investigations. In 2001, the F.B.I. confirmed the existence of Magic Lantern, a type of spyware that comes in an e-mail attachment. At the time, the agency denied that the spyware had been deployed. But in 2007 the F.B.I. obtained a court order to use a similar program, called a "computer and Internet protocol address verifier," or CIPAV, which works much the way that RATs do, secretly monitoring a computer's use remotely.

At CrowdStrike, Henry might not need to obtain a court order to use malware, depending on how it is deployed. However, he said that he has no intention of violating the C.F.A.A. "We don't hack back," he said. "We don't take actions that are illegal. I've been enforcing the C.F.A.A. for fifteen years, and I've put a lot of people in prison for violation of that law. So we're not doing that. But," he went on, "there are a variety of things we are able to do from a deceptive standpoint that don't involve putting malicious code on hackers' machines. Feeding them misinformation, giving them the wrong trade secrets. You can't give them the wrong plans for a plane, or the wrong drug, because people die. But if it's business plans, tactical information, it's different."

Orin Kerr, a professor at George Washington University and an expert in computer-crime law, argues that back-hacking could easily get out of control. He also told me, "It's hard to know if you are targeting the right person. It's easy to disguise your location online, so it's easy to create a false impression that someone else was behind the attack." But Stewart Baker, the former head of cyber policy for the Department of Homeland Security, maintains that in certain cases hacking back should be within a victim's rights. "If you had a motorcycle in your garage, and your neighbor stole it, and you could see a trail of oil leading from your garage to his garage, you're going to go get it back," he said. "And I don't think a court of law would convict you of trespassing. So, if you hack my intellectual property, shouldn't I be able to get it back?"

Most hacking crews have characteristic digital signatures, cryptography keys, and methodologies of attack, and all that information could be used to identify them, and possibly arrest them. But the information is rarely shared between the public and the private sectors. When the F.B.I. detects a cybersecurity breach at a company, agents show up at the door with guns and badges and inform the company of the break-in, but they don't reveal who the intruders were, or what they were looking for, because that information might compromise the F.B.I.'s sources and methods. And when a private company discovers a security breach on its own (on average, more than two hundred days after the initial intrusion), it generally doesn't share the information either with the F.B.I. or with the public, fearing the impact on its partners, investors, and customers. Even private companies operating critical infrastructure sometimes decline to cooperate with government investigations of cyber attacks on their facilities. "Some of these companies are government contractors—they work with us!" McFeely told me. "That doesn't seem right."

Alperovitch said, "Everyone is focused on malware in the security industry. But malware isn't really the problem. Organizations think they have a malware problem; in reality they have an adversary problem. Someone is coming after them for a reason. People say attribution is impossible, but there are two fallacies with that. If you are doing multiple attacks, over years, the possibility of attribution goes up. And the second thing is we bemoan the lack of privacy that we have online, but that makes it harder for an adversary to operate in cyberspace without leaving a huge digital footprint as well."

Adam Meyers, CrowdStrike's intelligence director, showed me a picture of a Chinese hacker who had penetrated one of its client's networks. CrowdStrike used the hacker's unique cryptography key to trace him back to a Chinese university, where it was able to identify him by name, and then find his picture on a social network.

Alperovitch pointed at the young man, who was wearing a tie and a short-sleeved dress shirt and leaning on a large rock with three Chinese symbols on it. "This makes it personal," he said.

A second picture, also taken from the hacker's social-network page, showed the man in military gear, posing with a squadron of other, similarly clad men.

"Looks just like P.L.A., right?" Meyers said. "We thought we'd hit gold." But, on closer inspection of the uniforms, it turned out that the men were dressed for paintball.

Looming darkly over this almost Mordorian cyber threatscape is the prospect of cyber war—a future conflict fought with weaponized code that can do physical damage to infrastructure,

and potentially kill people. So far, the only nations known to have deployed such code are the U.S. and Israel. Working together, the two countries produced the Stuxnet worm and, reportedly, Flame, a high-grade espionage tool. Stuxnet, discovered in 2010 but deployed as early as 2007, was designed to attack Iran's nuclear facilities by exploiting multiple zero-day vulnerabilities in Microsoft's Windows; it reportedly destroyed about a thousand of the centrifuges used to enrich uranium, by causing them to spin out of control. Iran is believed to have retaliated by launching many of the 2012 DDoS attacks on U.S. banks and by infecting the oil company Saudi Aramco with a virus that damaged tens of thousands of its computers, with the aim of impeding the flow of oil.

"This has the whiff of August, 1945," Michael Hayden, the former C.I.A. and N.S.A. director, said of Stuxnet, at an event at George Washington University in February. "It's a new class of weapon, a weapon never before used." A cyber arms race is getting under way, and it is escalating, as the tools needed to deploy weaponized cyber attacks spread around the world. (In March, General Alexander, of the U.S. Cyber Command, told the House Armed Services Committee that he's establishing forty new cyber teams, including thirteen dedicated to offensive attacks.) Whether that conflict will be "hot" or "cold" is hard to say, because virtually all the government's cyber operations against other countries are classified (neither the U.S. nor Israel has taken responsibility for Flame), cloaked in the same secrecy as our drone attacks. David Rothkopf, of *Foreign Policy*, recently characterized cyber conflict as a "cool war," writing, "It is a little warmer than cold because it seems likely to involve almost constant offensive measures that, while falling short of actual warfare, regularly seek to damage or weaken rivals or gain an edge through violations of sovereignty and penetration of defenses." In any case, the Department of Defense recently announced a fivefold increase in our national cyber forces.

And yet, dire though matters appear to be, the American public doesn't seem particularly alarmed by our cyber-security problem. Danger is everywhere and also nowhere; being invisible, cyber crime is easy to put out of your mind. In this respect, at least, it is nothing like terrorism, which feeds on bloody spectacles, martyred bombers, and public mayhem. The cyber threat is faceless and creeps in on little cat feet. You know that, like death, it's coming, but all you can do is hope that someone will fix it before it comes for you.

There is nostalgia in the voices of security people when they speak about the "good old days" of the nineteen-nineties, when the gravest threat to network security came from computer viruses. "Wasn't it nice?" Raimund Genes, Trend Micro's chief technology officer, said recently, waxing nostalgic about Melinda, the 1999 computer virus, which, along with the "I Love You" virus, of 2000, marked the end of the age of viruses and the dawn of cyber crime. "A virus was highly visi everyone knew something was wrong with the system. virus was just done for fun. There was no commercial in creating viruses."

Tom Kellermann told me, "Guys like me—I'm not ing this anymore. It's like I'm a forest ranger, and the day I used to have to deal with forest fires that we dentally set by campers, and now I have to deal wi that are set by arsonists." He added, "I'm looking a shit, crazier crap every day, running on four hours only ever seeing part of the puzzle, and everyone I k the government who deals with this is completely fr There's a multiplicity of actors, in a free-fire zone. tired of people saying China this and China that. If it w China, then at least we could create international nor use diplomacy and other mechanisms that have been for hundreds of years."

So is there any solution to our cyber problem? Every a in connectivity and mobility seems to increase the poss for crime.

"We're completely fucked," Kellermann said. "I bo new car yesterday. And the guy says, 'Hey, man, do yo you can turn on a Wi-Fi hot spot in your car?' I said, the?' He said, 'Yeah, it's constantly on, bro, so all yo to do is have any of your passengers synch their device and you can get high-speed Internet while you are driv said, 'Are you fucking kidding me? Where is it? Turn i

Critical Thinking

1. In what fundamental ways does cybercrime differ from traditional crime that makes cybercrime a threat our secu experts express worry about?
2. Seabrook says, "From the earliest days of the Internet, th approach to network security has been to play defense." what playing offense and defense means in this context? are examples from the article of each? What are the pros cons of each approach?

Create Central

www.mhhe.com/createcentral

Internet References

Cyber Crime: Nailing the Botnet
www.businessworld.in/news/finance/cyber-crime:-nailing-the-botnet/924848/page-1.html

Cyber Thieves Steal $45 Million [PBS NewsHour.]
www.pbs.org/newshour/extra/daily_videos/cyber-thieves-steal-45-

U.S. and China Leaders Debate Cyber Security [PBS News
www.pbs.org/newshour/extra/daily_videos/u-s-and-china-leaders cyber-security