Introduction

JOANNE MYERS: Good morning. I'm Joanne Myers, director of Public Affairs Programs, and on behalf of the Carnegie Council I'd like to thank you all for joining us.

Our speaker is Misha Glenny, who will be discussing his new book, entitled *DarkMarket: Cyberthieves, Cybercops, and You*. Written with the skillful pen that our speaker is known for, his latest book reads like a crime thriller as he tells the story of law enforcement's newest nightmare, the Internet.

Visions of a bright new future have long been linked to the increased use of technology. From H.G. Wells to *Star Trek*, the buzz about technological innovation has been, in part, of things to come.

Yet, not all that was envisioned has been for the common good. In the past couple of years alone, a series of shocking events have taken place in cyberspace that would have been difficult to imagine until they actually occurred. For example, the Chinese electronic break-in at Google, to the Stuxnet's worm stealthy attack on the Iranian nuclear program, to mass breaches of stolen consumer data, have shown us just how effective criminal activity can be in cyberspace.

Cybercrime, which is broadly defined as any crime that uses a computer, has become a global problem. It can take a variety of forms, and the implications for individuals, governments, and corporations are profound. Cyber activity knows no borders, which makes it much more difficult to identify when people are up to no good and extremely challenging to combat.

In *DarkMarket: Cyberthieves, Cybercops, and You*, Mr. Glenny explores the rise and fall of a single obscure website called DarkMarket. What he uncovered may alarm you, but these stories illuminate aspects of the problem while shedding light on related criminal exploits taking place in cyberspace.

Between 2005 and 2008, the site DarkMarket served as a premier destination for criminals engaged in online fraud. It was dedicated to facilitating the exchange of information, such as stolen credit cards extracted through scams from hackers, credit card swindlers, spammers, and other cyberthieves.

Mr. Glenny reveals how cybervillains face the permanent challenge of trying to establish bona fide credentials, how they develop methods to identify one another, and how police forces around the world have attempted to counter the hackers' ability to spot law enforcement agents and informants.

Over the past two years, our guest met the criminals and those who try to catch them. In more than 200 hours of interviews, he spoke to most of the major players on both sides of the law. In following these criminal trails, he discovered many things, but first and foremost just how difficult it is to police a crime that is so widely distributed

geographically. For example, money can be stolen by a Russian based in Ukraine from an American company and paid out in Dubai.

As our lives become ever more entangled with the web, *DarkMarket* reveals just how easy it is to become complacent about our personal security. And even though sites may be shut down, hackers caught, digital crime is everywhere, and it is growing. So next time you are inclined to share details of your lives, take money out from that ATM machine, or click on a questionable-looking email from your bank, you just may want to think twice, as you can't be too complacent when it comes to your personal security.

With that in mind, please join me in taking a tour of this esoteric underworld with our expert guide, Misha Glenny.

Thank you for joining us.

Remarks

MISHA GLENNY: Joanne, thank you very much. Thanks very much indeed. That was such a good and thorough introduction, I feel as though half of what I have to say may have been taken away from me.

But I will just start by explaining—because I don't want to deny you the unalloyed pleasure that you will have in reading the book, and so I'm not going to talk about exactly what's in the book today, but the whole sort of range of peripheral issues which the book throws out, but just to clarify, because it helps to sort of locate it, as it were.

DarkMarket, as Joanne said, was a website, www.darkmarket.com, and when you got there it was basically a forum, a members' forum.

Now, I don't know what the equivalent is here in the United States, but in Britain we have a very famous forum, called Mumsnet.co.uk, and Mumsnet is where, if you are a distressed parent of teenagers, say, as I am, you go on to Mumsnet and there is a whole series of things. There will be something like, "My 13-year-old daughter is on the pill, I've discovered; what do I do?" and then a whole series of other distressed parents will explain what you do when you find your 13-year-old daughter is on the pill. DarkMarket is the same format as Mumsnet; it's just it's for criminals.

So you sign on. But, obviously, you have to be vetted more thoroughly than if you're just a distressed parent, and I'll come to the vetting procedure a little later.

So you sign on, and then you have a row of things. Instead of teenagers, toddlers, and so on and so forth, you have viruses, credit card fraud, identity theft, and that sort of thing, and you sign on to read about those particular subjects, how to perpetrate the crimes. And, above all else, DarkMarket and its predecessors were, as Joanne said, a place where you could exchange information in order to carry out crimes.

The bulk of crime on the Internet, what we call high-volume/low-impact, is credit and debit card fraud. So about 60 percent of you here in this room will have had your credit or debit cards compromised at some point over the past five years, whether you know it or not. That is because it is very easy for criminals to get hold of credit card details, store them electronically, and then sell them or use them in ATM machines around the world.

The reason why DarkMarket and its predecessors were so successful is that the original criminal forum, which was founded—perhaps appropriately, as we may discover later, in Odessa in Ukraine in 2001, called CarterPlanet.com—the original forum came up with the answer to the fundamental challenge posed to criminals operating on the web. That fundamental challenge is: How can I trust the person I am doing business with when, as a criminal, it's axiomatic that they're untrustworthy? This is quite a conundrum.

CarterPlanet came up with this brilliant idea. It was run by five administrators, who called themselves, rather unimaginatively in my opinion, "the family." One of the family was designated as the escrow officer. The escrow officer was an independent arbiter. So, essentially, playing the role that is the essence of mafia organizations, what they had been playing since the middle of the 19th century, when the mafia first emerged as a social and economic force in western Sicily.

So what happens is that I am a criminal and I've got 5,000 credit card details that I want to sell roughly at around $7-$8 a pop. So that's quite a lot of money. I send my 5,000 credit card details electronically to the escrow officer at CarterPlanet and the potential purchaser sends the money to pay for those digitally also to the escrow officer. So the escrow officer has both the credit cards and the money in his possession.

And I use the gender advisedly. Throughout this talk we will be talking about men and not women. Ninety-five percent of hackers are male.

The escrow officer then sends a random sample of the credit cards to his friends around the world—in Rio, in Toronto, in Wellington, in Dubai—and they go and use the credit cards in ATM machines. If they work, they are allowed to keep the money and the escrow officer is allowed to keep the money as a fee for the service. If it works, he then releases the credit card details to the purchaser and the money to the vendor.

This in 2001, when it was devised, led to a "champagne period" of crime on the Internet and beyond, because banks at this point and financial institutions and companies had no idea—some would say even no interest—because they were so obsessed about making huge sums of money through speculative practices on global markets that the money lost to cybercrime was simply not sufficient for them to register on their complex networks. But that's by the way.

So that's what DarkMarket was. It wasn't just for credit cards; you could also buy and sell viruses, as I said; you could buy and sell identities; if you needed a passport from any country in the world, you could buy it in DarkMarket; and so on and so forth.

So how did I get to DarkMarket in the first place? Well, around 2006-2007, when I was researching my book, *McMafia*, on global organized crime after the fall of communism, I went to Brazil.

I went to Brazil because—well, partly because the place I had been to just before Brazil to research *McMafia* was Dubai, and that was one of the most soulless experiences in my existence. It is particularly difficult to get anybody to talk on the record about anything in Dubai because everyone is frightened of being thrown out of the country. So it was a very difficult research environment when everyone kept quiet.

So, after that, I went to Brazil, and of course it was the polar opposite. You go to Brazil, and you cannot stop people talking. It doesn't matter whether they're police, whether they're criminals, whether they're intelligence agencies. They just go on and on and on. And, of course, they like to party. It was absolutely wonderful.

Within about five minutes, I had stumbled across a group of criminal hackers in Brazil because, interestingly, Brazil, along with Ukraine and Russia, was one of the great incubators of cybercrime. The BRIC [Brazil, Russia, India, China] countries have a very special role to play in the world of malfeasance on the Internet.

These young Brazilian criminal hackers—and again, we said "male" before; now we use the word "young"—the guys that I met were all under the age of 20 at the time—they were part of an operation, which the police in Brasilia had dubbed Operation Pegasus, in which over a three-year period they had succeeded in stealing over $200 million through a very sophisticated Internet scam.

Four of the group had been arrested and were in prison. But I managed to meet two of the group, and one of them in particular, after the police had sort of given up the investigation, more or less. This one guy explained to me exactly how this thing took place and how these teenagers were able to make such vast sums of money.

I then went to the police in Brasilia who had arrested the four people in Operation Pegasus and got their side of the story.

Then, in order to get a sort of independent sense of what was going on, I went to visit the São Paulo branch of something called ISS [Internet Security Systems], which is a security company based out of Atlanta, Georgia, that is now owned by IBM.

At ISS I happened to coincide, fortunately, with a visit from the head of ISS's special investigation team, a man named Peter Allor, who, like so many people in the private security computer world, was an ex-government agent. He was head of a cyber unit in the CIA.

Actually, the strange thing is, when you look at security at companies like Google and Microsoft, Yahoo!, and all these sort of touchy-feely West Coast companies which are all about not doing evil and things like that, if you look at their security divisions, it's all ex-

FBI, ex-Secret Service, ex-DEA [Drug Enforcement Administration]. They're all totally ruthless, these people.

Just as an aside, in terms of your tax dollars, your tax dollars are spent to invest a lot of money in training up these people at the FBI and at the Secret Service until they've just got to the level of super-cyber investigators, and at this point in come the recruiters from the West Coast and say, "Why don't you come and work at Google, and, instead of paying you $90,000, we'll pay you $900,000, and you live on the West Coast and you don't have to live in Washington."

And, of course, every single one of them goes over to the West Coast, your investment of course having been made into the government agent training program first of all. But that's just a side issue.

Anyway, so I met Peter Allor, a fascinating guy. Slightly socially autistic but incredibly good at laying out what was going on in cyberspace. I had never heard anything like this at all in my life, about this "arms race" between criminals and between security companies and law enforcement agencies that had proliferated all over the world, that had started in places like Brazil and Ukraine and Russia but was now happening everywhere, and each new emerging economy zone brought with it a new rush of young criminals who are incredibly entrepreneurial, energetic, and very, very smart.

As a consequence of that, I went to visit ISS's headquarters in Atlanta. The centerpiece of ISS is their control room. It's absolutely astonishing. You walk in, and it's just like going into the bridge on the Starship *Enterprise*, where you have all these chairs sitting around with people swiveling around like that without saying anything. One of them has got a pony tail, the other one has a lot of spots, and the third one is an Asian-American, and they are all sitting there going like this.

In front of them are four huge screens with data going across the screens all the time. I was told that these are the actual real-time attacks on all of their corporate plants around the world. So you have Toshiba up on the right-hand side, you have Volkswagen in the middle, and these guys are sitting there warding off these cyber-attacks the whole time. They don't say anything. Personally, I found it fascinating, but ten minutes in there and I'd had enough.

But of course I'm not the sort of person—you wouldn't believe some of the people involved in computer security. You know how sometimes you go home with a good novel and sit down and you read a good novel? Well, they go home with books—I kid you not—full of computer code, and they just sit down and they read this computer code as though it were a good novel. It's quite extraordinary.

So it's a totally different world. But you start to get used to it and assimilate it. That was one of the places, ISS, where I began to do this.

So I realized from Brazil that things on the Internet were going completely wild and that after the organized crime book I would have to do something on the Internet and what's going on on the dark side of the Internet.

Now, the first thing that you learn—and I learnt this from Operation Pegasus—is that actually the great majority of crime that takes place on the Internet is not to do with individuals' technical ability.
Hacking plays a very important role, but it's only—and this is a guesstimate, but a guesstimate based on having worked on it for the past two or three years—real hacking ability accounts for about 20 percent of crime that goes on on the Internet. Eighty percent is accounted for by what we refer to in the trade as social engineering.

Social engineering is the act of persuading individuals to do things on their computers which are objectively not in their interest, but they don't know that. So clicking on a link, for example, which will actually take you to a website that, say, downloads a virus onto your computer, and your computer then either downloads a key logger so that everything you type on your computer is being tracked by somebody else, including your passwords to your bank, to your email account, and so on and so forth.

Or, for example, a virus which will subordinate your computer's computing power to a command-and-control unit somewhere elsewhere in the world, and that command-and-control unit can order your computer to do whatever it wants.

Usually, that means that your computer will become part of what we refer to as a botnet, which is thousands, tens of thousands, of computers controlled by one computer which is then able to order the computing power of those 10,000 computers to attack a website, to attack a company system, or something like that. This is all going on without you having a clue. You know, you're merrily saying, "happy birthday," sending an email, and that sort of thing. You don't know.

But of course, first of all, the criminal has to persuade you to click on the link so that you download the virus. So how do they do that?

Well, of course, they worked out very early on that the fastest way to persuade somebody to do something stupid on their computer is to offer them a promise of sex or love. You know the Internet of course is a boon for the pornography industry, but it is also a boon for the criminal industry because of the boon for the pornography industry.

I don't know if you remember, but one of the first viruses which spread around the world like wildfire—this was actually in 2001—was called the ILOVEYOU virus. You got this email, and the headline was "I love you . . . " Then, inside the email it says "click on the link to find out who loves you."

Of course people, we're all humans, we all want to be loved. And, even if we're in stable marriages for 15 years, or in fact because of the fact we've been in stable marriages for 15

years, when somebody says, "I love you," you say, "Who is it? Who loves me?" So everyone clicked on that.

Now, I was very fortunate when the ILOVEYOU virus came along, because the first person I received it from was my ex-wife. [Laughter] She harbored all sorts of emotions towards me, but love was definitely not amongst them. So as soon as I saw this email from my ex-wife saying, "I love you," I said, "Oh, no you don't." So I knew it had to be a scam. So I was able to put it in the electronic trashcan and saved myself a very nasty infection.

So do be careful about what you click on, because that's how cybercrime is essentially perpetrated.

We are all vulnerabilities. We are the ways in which cybercriminals can get into computer systems. So, unfortunately, we have to learn how to change our behavior.

Now, every time you see a new iPad come out or a new series of mobile phones, what is happening is that for the people who want to penetrate computer systems these are new possibilities and new entrances.

It's very interesting. If you talk to people from the World Bank or from development organizations about the fact that fairly soon we are going to have a fiberoptic cable running down the east coast of Africa, the World Bank official will say, "This is absolutely fantastic. This is going to be terrific for development of East Africa and we should all invest in it."

If you talk to an officer of the FBI and say, "How do you feel about the fiberoptic cable running from Kenya down to Tanzania?", they put their heads in their hands and say, "This is going to lead to a burst of criminal activity on the Internet."

So everything that happens on the Internet has pluses and minuses.

So you have the social engineering business, and then you have these characters, the hackers, who have an extraordinary ability to break into computer systems.

One thing that I have been looking into that emerged out of *DarkMarket* is about the psychology of hackers. What is it that motivates hackers. What do we know about hackers?

It's interesting. I did a little bit of research recently on how much money we spend every year now on cyber security. Around the world—excluding Russia and China, who also have their own very big spend but they don't publish it—around the world we spend $120 billion a year on cyber security, of which about 60 percent is government spend on cyber security, and of that 60 percent government spend, about 40 percent is accounted for by the United States of America. So these are huge sums of money, which are scheduled to double in the next five years or so.

What do we actually spend that money on? We spend that money on what are called high-end digital solutions, which means you get companies like Lockheed-Martin, Northrup Grumman, Raytheon, and you pay them large sums of money, and they come in with these incredible whiz-bang systems to prevent you from coming under attack from hackers, which will work up to a point; but there are few, if any, systems around the world which are 100 percent secure.

But, interestingly, what we don't do is we don't spend any money on researching who the people doing the attacking actually are—where they come from, what their socialization process is, what their motivation is.

This is important because so far I've been talking to you about cybercrime. But in order to understand what is going on on the 'net, you have to think of three pillars, what I call "the three pillars of malfeasance" on the Internet:

- There is cybercrime, which is your credit card being nicked.
- There is cyber industrial espionage, which is companies seeking to break into other companies' computer systems in order to use the data in the computer systems to gain a competitive advantage. That accounts for about 34 percent, according to Verizon's latest threat assessment. Thirty-four percent of bad stuff on the 'net is company-to-company things, which nobody ever reports because nobody likes to admit that they have been the victim of a successful hack attack. They admit it to Verizon every year, but anonymously, and that's where Verizon gets their data from.
- The third thing is the big one, is cyber-warfare, state-to-state warfare or nonstate-actor-to-state warfare.

And of course, as Joanne mentioned, we have seen the emergence in 2010 of this virus called Stuxnet. Stuxnet was a game changer.

The whole environment that we exist in digitally has now changed because Stuxnet required something in the region of a ten-person team—I think we can safely assume that it was a ten-man team—six months to develop this virus. This virus was aimed very specifically at a complex industrial plant developed by Siemens, and very specifically at a part of that plant, to wit, the motor that pumps the water around the system. And it was aimed very specifically at uranium-enrichment facilities in Natanz and Bushehr in Iran.

Now, the reason why it's important is not "Was it the Israelis, was it the Americans, was it the Chinese?", which is the sort of political debate going on behind it. Nobody knows for sure who it was, except for those who perpetrated it, and probably American intelligence as well knows who perpetrated it.

But what's important is less the sort of political speculation and more the fact that somebody put all that effort into developing this very specific virus and then deployed it, and by deploying it, whoever they were were standing up and saying, "Not only do we

have this technology but we are prepared to use it in nuclear facilities." And it could have resulted in a nuclear accident.

As soon as that happened, every state around the world said, "Wait a minute. This is getting really serious. We have all got to start developing our cyber offensive and defensive capability."

Since 2010, we have been involved in a relatively unrestricted arms race, which before was largely restricted to the United States, Russia, China, Israel, France, Germany, and Britain. We now have a relatively unrestricted arms race, with lots more people coming in developing their own cyber-offensive capacity. Hezbollah in Lebanon, for example, has its own cyber development unit, and one or two other places. Iran, obviously, is working very hard on this as well. India is working very hard on this.

This is all taking place outside of any international treaty or framework. That is because we have very different perceptions of what the Internet should and shouldn't be.

The Chinese believe that restrictions should be placed on this part of the Internet—basically, you can't talk about various subjects in China on the Internet. The Americans think that restrictions should be placed on this part of the Internet—i.e., you shouldn't be allowed to download Hollywood movies before they have reached the theaters. Because of that, no one can agree on what the regulation of the Internet should be.

What we have seen over the past five to ten years is that states all over the world are, whether citizens like it or not, beginning to regulate the Internet, and in some cases with fairly Draconian laws, as we have seen in places like Syria and Iran. Russia has a very extensive monitoring capability over its Internet, and so on and so forth.

So there you have those three pillars, which, if they were all separate and that you knew that the FBI was looking after cybercrime and you knew that the private sector was trying to combat cyber industrial espionage and you knew that the military was trying to keep a damper on cyber warfare, that would be all terrific. But, unfortunately, the great genius of the Internet, its interconnectedness, is also its Achilles' heel.

You have people who may be involved in cyber warfare working on sites like DarkMarket. So when I was researching DarkMarket, the number of times that I came across intelligence agents hovering around DarkMarket to try and see what was going on was astonishing.

I came across people from Turkish domestic intelligence, I came across people from the FSB [Federal Security Service of the Russian Federation] and the SBU [Security Service of Ukraine] in Russia and Ukraine, I came across people from MI6 [Secret Intelligence Service, UK]. And there's not a criminal website in the world that the National Security Agency doesn't know about and isn't looking at; the same with GCHQ [Government Communications Headquarters] in Cheltenham in the United Kingdom.

The reason for that is that hackers migrate between the three pillars.

You may be a hacker working for an insurgent or terrorist organization that is using DarkMarket as a revenue-raising operation. You may be somebody who is working on cyber warfare techniques who is using DarkMarket to see what viruses are coming out in the criminal world, because, with something like Stuxnet, some of Stuxnet was cobbled together from existing viruses that were common in the criminal world. Everything is becoming this sort of cacophony in cyberspace in the security sector, which is made all the more difficult by the fact that you never know who you are dealing with.

This is why I am beginning to argue now publicly and in law enforcement and national security arenas for some of the $120 billion a year that we spend on whiz-bang solutions to Internet security to be channeled into researching who hackers are and what they are doing.

At the moment, we have a very simple rule in the Western world, and that is, if anyone exceeds their authorized access—and that's the phrase used in the Computer Fraud and Abuse Act here in the United States—then they are criminal. And it doesn't matter what they are doing. If you are a member of DarkMarket trying to hack into a computer server in order to secure financial gain, you are the same as a youthful idealist who works for Anonymous hacking into Stratfor, for example.

But it's interesting. When we look at something like Anonymous, which is a very, very curious phenomenon, they're a new political movement with an ideology—in my opinion a fairly half-baked, semi-anarchic ideology—an extraordinary ideology, which doesn't just attack Stratfor and PayPal and defense of Wikileaks and things like that. Other targets of Anonymous have been the Mexican drug cartels; Boko Haram, the Islamist insurgency in Nigeria; and Greek oligarchs who are trying to make a quick buck out of the crisis in Greece. So they are tapping into a real idealism of youth.

Yet, according to us, in terms of law enforcement, they are all criminal hackers who should be in jail. I think we need to think a little more carefully and research into what is happening to young people that is leading them to resort to this type of activity.

I'd like to demonstrate this very briefly by telling a story about my daughter, who is 19 years old. She's very sweet, but she's pretty feckless on some occasions. She lives with me. But she was going to stay one evening with my ex-wife, the same one from whom I got the email, because she was going to take her to the airport the next morning very early. She left our house at 6:00 pm in the evening and off she went. I said, "Bye-bye, Sasha, have a lovely time."

Then, at 1:13 in the morning, I get a call from my ex-wife saying, "Where is she?"

I said, "What do you mean? She left here at 6:00 pm." She's 45 minutes away on the subway, on the Underground.

My ex-wife said, "She's not here. Her phone is turned off. I don't know where she is. We're leaving for the airport in three and half hours' time. What's going on?"

I said, "I'm sorry, I don't know." I tried to ring her—nothing, and so on.

So a little bit of panic ensued at this point. I decided the only way that I could get hold of her was by hacking into her Facebook account. So I got to her Facebook account, I got her user name, and then I put in her password.

Now, how did I know her password? Well, six years ago my daughter had told me, as a 13-year-old, the password that she uses for her Hotmail mail account. Sure enough, six years later she is still using the same password for all of her accounts everywhere, which is the sort of 1.01 big fail on cyber security, is don't use the same password because your father can hack into your Facebook account as a consequence.

So anyway, we discovered—the extraordinary thing is this was 3 o'clock by now on a Monday morning, and what is really shocking is that at 3 o'clock on Monday morning half of Sasha's friends on her Facebook account are up there chatting at 3 o'clock in the morning, the most extraordinary inanities. You wonder sometimes what is happening to the younger generation. But that is, as I say, by the way.

I put out this message saying: "This is not Sasha. This is her father. She has gone missing. If any of you know where she is, please get in touch with me or her mother. Here are the phone numbers."

And sure enough, within half an hour she had rung her mother. She was too scared to ring me. She didn't speak to me for two weeks because she went off on holiday for two weeks.

When she came back, she finally deigned to speak to me again. She was speaking to me because she had got over the fact that her behavior was so bad. But after two weeks she was still livid that I had hacked into her Facebook account. She was really angry.

If any of you have experienced teenagers on Facebook, you know they will tell the rest of the world absolutely anything. They'll tell them about how often they get drunk, whether they are taking drugs, what they think of their teachers, and so on. But their parents are not allowed to know any of it. So she was really angry that I had hacked into it.

Now, if we had lived in the United States and she had not only been feckless but vindictive, she could have taken me, under the Computer Fraud and Abuses Act here, and taken out an action against me which could have resulted in me being imprisoned for three years for having "exceeded my authorized access."

That is the situation at the moment. We do not have any leeway legally for understanding whether a hack, unless it is sanctioned by a state agency, has some mitigating circumstances to it or not.

We are moving into a period where the state is arrogating ever more rights to itself in terms of who can and who can't do what on the Internet. What we are seeing is a response, particularly from the younger generation and from the so-called activists like Anonymous—we are actually seeing real resistance to this. It is a new form of political struggle that nobody has really begun to order. We don't really understand what is going on on the Internet.

I think it's high time that we started looking into why a lot of hackers are males who begin their work aged between 12, 13, 14, and 15; why so many of them have advanced abilities, if not gifts, in math and sciences; why a significant proportion of them have underdeveloped social skills; and what it is about the community in the Internet that liberates them in a way that no other environment has ever done. But, instead, at the moment what we are doing is, rather than looking all this sort of stuff, we treat them like criminals.

If you listen to the hack that Anonymous did ten days ago on the FBI conference with the Metropolitan Police over the telephone, which is an absolutely fascinating thing, all the cases that they are discussing are of teenagers—one is 19, but the rest are all 15 and under. It's like they are talking as though they are just "bog down" criminals as we say, to use the English phrase.

This just isn't enough, it seems to me. I'm not saying that the FBI isn't doing a good job or anything like that. They have their job. It's very clear.

But there are so many strange, bad, and dangerous things happening on the Internet that we now have to start looking at it as a mature society with a need for investigation, research, data, and so on and so forth, because if not we are going to run into trouble.

That I say because our potential competitors are all using hackers, whether it's the Russians, the Chinese—the Israelis may not be potential competitors, but they certainly use their hacking ability, which is why they only have a population of about 8 million but they have a cyber capacity out of all proportion to their population.

It's time we started getting real about what is going on in the virtual world. Otherwise there will be real problems facing us ahead.

Thank you very much.

Questions and Answers

QUESTION: Richard Valcourt, *International Journal of Intelligence*.

Richard Clarke, in particular, has warned that despite all the protective measures that are being taken, with the Microsoft software being used almost universally, it is almost impossible to guard against any kind of hacking. So what has your research shown regarding the bypassing of Microsoft for security purposes?

MISHA GLENNY: Well, the first thing it demonstrated to me is that, as I said earlier, cyber security is not about the elimination of risk because you cannot eliminate your risk. What you can do is you can massively reduce your risk.

If you are an individual consumer, the quickest way to massively reduce your risk is to dump Windows systems and go over to Apple. That is not because Apple are intrinsically better systems when it comes to security. It's because people involved in bad stuff on the web are rational human beings and they do not develop viruses and other hacking tools for systems which only account for 5 percent of the global networked computer systems. Just under 90 percent is accounted for by Windows. And so you go where the money is. So that's your first problem.

It is likely to change over time because of the popularity of iPad and iPhone, in particular, as we migrate over to mobile devices as the primary way of accessing the Internet.

But, in principle, Dick Clarke is correct about this. I have to say that within the pantheon of those security people dealing at this level with IT security, Dick is on one of the far extremes, and that is "the world is about to fall on our head and it's going to happen tomorrow." He talks about "Cybergeddon" or "digital Pearl Harbor," when imminently planes are going to fall out of the skies, metro trains are going to fall off the Brooklyn Bridge, or whichever bridge it is they go over, and all that sort of thing, because out networked computer systems will be attacked.

You have then at the far end people who say that the whole security industry is the invention of the security industry and all the threats are the invention of the security industry because they're just doing it to make a whole load of money.

It seems to me, after looking at this for three years, that the sensible position to be is really in the middle on this one, that there is no doubt that some threats are hyped up because people can make money by hyping up the threats.

But to imagine that there is no security threat on the Internet is simply to close your eyes to everyday reality. All you have to do is to put a Windows system onto the Internet. You don't have to surf the web or anything like that. You just put it onto the Internet without any antivirus software, and within a matter of two or three hours there will be viruses crawling all over that computer. So end of story in terms of is it a threat or not.

There is no question about it, the Microsoft systems are incredibly successful commercially. But they represent a threat.

Some of the viruses have been seen on major infrastructural things. When you had a blackout in New York, whenever it was—a few years ago; I've forgotten when it was—they looked at the computer systems afterwards. There were viruses there which didn't cause the blackout but which made rebooting and getting the systems back up and running more difficult at the time. So that was evidence that the viruses were there.

More frightening than that was the fact that, as revealed recently by *Wired*, some of the drone planes based out in Nevada, the ones which bomb Pakistan and Afghanistan and are driven by 17-year-olds in Nevada, that the new-generation drones have been infected by viruses. Although the Pentagon has tested them and these viruses are not actually doing anything, they are there, and they can't get rid of the viruses. That is very, very disturbing, when one of your main attack weapons is vulnerable to computer viruses. This was a Windows-based system.

There's one thing I didn't mention, by the way. After 2010 and the Stuxnet and one or two events that happened before that, and that is that the United States established the U.S. Cyber Command. That means that the fifth military domain has been established, after land, sea, air, and space. And, interestingly, it is the first ever manmade military domain.

It is no coincidence that the commander of Cyber Command, General Keith Alexander, is also the head of the National Security Agency. This is a recognition of the fact that military and intelligence in the cyber world are very, very difficult to deconstruct, to disentangle.

Now, if you are here in the United States—sorry I'm going away from your question, rather, but it has provoked a number of thoughts—the threat from cyber big time is from Russian criminals and the Chinese involved in espionage all over the place. And they are. They steal everything they can and they don't really care about it. For the most part it's really not that important. So it feels like the United States is in a vulnerable position.

But if you look at the digital landscape from the perspective, say, of Moscow or Beijing, then things look very different indeed.

First of all, the United States has control over the two largest depositories of personal data in the world—to wit, Google and Facebook. If you are an FBI officer or a CIA agent and you get a court order from a federal judge, you can look at any part of that personal depository of data in Google or Facebook, any part you want, within 24 hours.

If you are a British officer of the Serious Organized Crime Agency in London, which has very close relations with the FBI and other law enforcement agencies in the United States, you have to apply for it through the courts, and maybe, after four or five months, you will get access to the account that you are looking at, by which time it will probably no longer be relevant in operational terms.

If you are a member of K Division of the FSB or you are a cyber officer in the People's Liberation Army in Beijing, you can whistle Dixie. You have no chance of accessing that data through legal means at all. So what do you do? You hack it. What else can you do? Because they look at the Americans and they say, "This is a huge strategic advantage."

And then, when you put next to that the digital reach of the National Security Agency in coalition with GCHQ in Cheltenham and the Canadian, Australian, and New Zealand

intelligence agencies, you realize that Americans' digital reach far outstrips that of any other country in the digital world.

And so this is a contested area. It is not simply a question of the United States under attack from bad people all over the world. When we are in these very beginnings of the discussion of "Can we have an international regulation for the Internet?", it's one of the things that you will hear repeatedly from the Chinese and the Russians, is, "Yes, but we want a level playing field too."

QUESTION: Warren Hoge, International Peace Institute.

One of the reasons I think that individuals don't take the kind of responsibility that you think they should for cybercrime is that it can appear to be a victimless crime. I get a communication from my credit card company asking if I was in Sofia, Bulgaria, last week and if I purchased a load of pashmina scarves and Cartier watches. When I say I haven't been in Sofia for seven years, I am instantly made whole by the credit card company, and the next day in the mail comes a replacement card. How am I individually victimized by such action?

MISHA GLENNY: Because the banks, who are the only sector of industry who keep a close track on how much money has been lost to cyber—they don't tell anyone. They don't tell the police. They certainly don't tell the customers. The one other industry that they do tell is the insurance industry. It is only in banking, but in no other sector, that there is any idea of how much money is being lost to cybercrime. That is because of their relationship with the insurance industry. They insure themselves against attacks.

In any other corporate sector there is no secondary insurance market to protect yourself against being hacked. But it does work in the banking system. They get the money back from the insurance company.

As the level of losses to cybercrime goes up, the insurance companies put up their premiums. The banks, who of course don't like to pay for anything, pass it on to us in the form of charges.

I've looked at my charges on NatWest at home, the bank that I work with, and they have been going up at a staggering rate over the past five to ten years, mainly the past five years. That is because we are all paying for cybercrime.

So it's not a victimless crime. It's particularly not a victimless crime.

There was a case two years ago of a woman, called Emma Woolf, who banked with Santander in London, which has only just been resolved. Santander absolutely refused to accept that she had been a victim of cybercrime, even though she had never used her credit card and kept it locked up in a drawer in her house. Her life was made a misery for the next couple of years. Then police uncovered a fraud within Santander and discovered,

purely by chance, that this fraudster had actually perpetrated the crime against Emma Woolf as well.

So it can sometimes turn very, very bad for you.

There's one case which I have to tell you about, which is the case of a man named Roger Mildenhall. He was an Australian living in South Africa whose case I researched when I was doing *DarkMarket*. In 2010, he got a call from a friend of his in Perth, which is where he was from, saying, "Roger, I can understand why you sold the first house, but why are you selling the second house?"

Now, he had two houses in Perth, which were his pension. His response to this was, "What do you mean I've sold the first house? I haven't sold either of the houses."

They said, "Yes, you did. You sold it two months ago."

What had happened is that his email account had been hacked into by a group from Nigeria and they had found on his email account copies of the title deeds to his two houses. They had then sent these to a local real estate agent in Perth and instructed the real estate agent to put the first house on the market. It was then sold for $350,000 and the money was transferred to China from where it was laundered.

Now, his life has been just a complete misery as a consequence of this. They managed to stop the sale of the second house. But even so.

Who is responsible for investigating that crime? Is it the Nigerian police, because that's where the attackers came from? Is it the South African police, which is where he was when it happened? Is it the American police, because it was a dot.com email account and so that comes under U.S. jurisdiction? Is it the Australians, where the houses were? Or is the Chinese, where the money was laundered?

The answer is of course basically it's no one, because when you are looking at something like Internet crime and Internet fraud, the global jurisdictions commit the crime but we remain restricted in law enforcement to local jurisdictions.

The only slight exception to that is the United States, where the United States claims jurisdiction anywhere if dollars are involved in the transactions or a company registered in the United States with a dot.com address is involved, which is why that email account was relevant.

So if you are a victim of identity theft, it can be utterly destructive to your life.

QUESTION: Susan Ball.

Has anybody tried to reverse-engineer or reverse-hack into Anonymous or DarkMarket?

MISHA GLENNY: Oh yes, they do that all the time.

QUESTIONER: Oh, okay, so they know what's going on.

MISHA GLENNY: In this world you can still, if are an advanced computer user, pretty much mask your identity, your location, from anyone. But you have to be an advanced computer user to do it, A). And B), you have to constantly check whether all your various systems, because you go through various tunnels and proxy sites and so on, whether they are all functioning properly, because one little slip-up and you can be found.

In terms of Anonymous and their sister organization LulSez, we had two fairly high-profile arrests in the United Kingdom, one in Essex and one in the Shetland Islands, and they are both awaiting trial now, which is likely to take place in May. They were tracked down by the Serious Organized Crime Agency in this case. The FBI has made arrests here. Spanish police have made arrests there. The Dutch police have made arrests there. So yes, it is.

What is interesting is that whilst some of the arrests of these characters from Anonymous were hailed as the bringing down of the kingpins, it doesn't appear to have impacted on Anonymous' capacity to undertake all sorts of attacks, including the deeply embarrassing recording of a confidential conversation between the FBI and the Metropolitan Police. They have become, it seems to me, ever bolder.

One of the interesting things about them is whilst they are international, they are also nationally based. So you have Anonymous.br in Brazil, you have Anonymous.at in Austria. Anonymous Syria is an incredibly active operation supporting the opposition in Syria in very practical ways, in masking where some of the opposition leaders are and things like this. So this is why I think that they are not simply just a group of overeager spotty kids who need a slap on the wrist, that they are actually a more interesting phenomenon than that.

But yes, they have been reverse-engineered and some of them have been arrested. But they don't appear to be down and out.

QUESTION: A number of years ago here at Carnegie Council we had a speaker [Stephen Flynn: America the Vulnerable] who warned us about our vulnerabilities militarily. Some government agency provided a team of hackers with some computers and a relatively small pot of money and sent them out to see what kind of damage they could think up in a few months. Within a few weeks they came back and announced that they had been able to open the locks on dams, to divert trains, to shut off power plants and water supplies. Are we still vulnerable to that or have things improved?

MISHA GLENNY: You'll find that it's a very mixed bag. In some areas things have improved. In some areas things haven't improved. What is the reason for that? The reason for that is what you are talking about is the critical national infrastructure.

Now, very recently I was at a conference at Ditchley Park in Oxfordshire, which is the FCO's [Foreign and Commonwealth Office] version of *Downton Abbey*. It was basically a group of spooks—defense department, MOD [Ministry of Defence], law enforcement, and everything. Everyone was sitting around for two days saying, "What do we do about the cyber threat?"

On the day that I was there, I was in this one working group, which was called Defining the Critical National Infrastructure. Around the table were about ten people, most of whom spend every waking hour of their lives trying to define the critical national infrastructure.

After eight hours of discussion, we had failed to come to any working definition of the critical national infrastructure. We had begun to look at priorities—telecommunications is actually the key priority. So you're trying to work out how long can you do without telecommunications, how long can you do without electricity, how long can you do without the logistics that ensure food distribution, how long can you deal without water, and so on and so forth; i.e., what is your resilience capacity?In that sense you prioritize the critical national infrastructure. But we've only just begun to get to any sort of working definition.

Now, 90 percent of the critical national infrastructure is owned by the private sector. So yes, the state can discuss what the priorities are, but the state can't necessarily monitor whether the private sector is meeting its obligations, or indeed what those obligations are. So this whole area is fraught with difficulty.

In the United Kingdom at the moment, there is a big thing of trying to get undercover. We have something called the Office of Cyber Security now attached to the government office, which is there to work out whether each government department is doing the right thing about cyber security.

It's a bold and beautiful attempt. But it's a complete hodgepodge because different people have introduced different systems; people don't like to talk to each other about their security because they don't trust the other person that they are talking with in different government departments, between different companies.

And companies are very reluctant to hand over information to government, not necessarily because they feel they should have rights and control over government, but simply they don't trust government with their data. This is another issue that we are having in building a cyber security structure, is that both government and the private sector have very poor records on handing out very sensitive information on CD-ROMs—left on trains and things like this all over the place.

The upshot of that is you will find some companies are very well run and have managed to integrate the whole culture of cyber security from the bottom up to the board level, and they are performing better.

But a lot of companies, both inside and outside the critical national infrastructure, in particular because board rooms tend to be aged over 55 and over and they see that this is a technical issue—"Just give it to the tech department."

They don't understand that it's not just about technical departments; that the greatest vulnerabilities in corporations here in the United States or in Western Europe come from two sources: outside contractors and disgruntled employees. So that means it's not just a question of technical; it's a question of human resources, it's a question of how you manage people, and so on and so forth. None of that really on a large scale has got through to the boardrooms yet.

JOANNE MYERS: I knew that if we trusted you to educate us about the Internet we wouldn't be disappointed. It was a wonderful morning. Thank you so much for coming.