THE EVOLUTION OF CYBERCRIME: FACULTY OF OTHER

IS THE EMAIL OF THE SPECIES STILL MORE DEADLIER THAN THE MAIL

"Cybercrime and Digital evidence" Conference at the Faculty of Law, Ljubljana, Slovenia

Professor David S. Wall, School of Law,



Leeds in the United Kingdom

WHERE I AM FROM

....

University of Leeds

LALLE





A brief synopsis of my talk – N.B. The title paraphrases Rudyard Kipling's poem "Female of the Species" (is more deadlier than the male).

➢Most cybercrime offenders find their victims through emails – respondents reply to content or unintentionally download a virus from an attachment. *Email replaced the mail used by fraudsters.*

>In recent years the increased volume of personal and corporate commercial traffic online has raised the value that can be stolen, which has triggered more sophisticated forms of victimisation.

➢ Viral attachments are being replaced by links to toxic websites from which recipients unintentionally download malicious software – usually via a flaw in their browser software.

➢Email is still a major source of infection, but not solely, some websites of reputable retailers have, for example, been compromised so that visitors become infected when visiting them.

>Email is still more deadly than the mail, but things are changing.

- PART 1 How has networked technology transformed criminal behaviour?
- PART 2 What recent developments in cybercrimes are continuing to challenge criminal justice systems. Two examples.
- PART 3 What developments in networked technology could initiate future online crime.
- PART 4 How do we regulate Cybercrimes?

PART 1 How has networked technology transformed criminal behaviour?

- It creates cybercrimes they are different to conventional crime (spatial, temporal, jurisdictional)
- Network technologies <u>change the nature of the</u> <u>organisation of crime</u> – They are force multipliers
- a) One person can control the criminal process
- b) They give access to victims across networks
- c) They give access to victims across a global span
- d) They make criminal activity more efficient



a) €50 million bank robbery

a) €50 million bank robbery

Complex organisation – Many people, inside knowledge, where, when, what resources, from where obtained?

a) €50 million bank robbery

- Complex organisation Many people, inside knowledge, where, when, what resources, from where obtained?
- Very risky, leaky intelligence, getting caught is inevitable, could go wrong – high risk & low return on investment

a) €50 million bank robbery

- Complex organisation Many people, inside knowledge, where, when, what resources, from where obtained?
- Very risky, leaky intelligence, getting caught is inevitable, could go wrong – high risk & low return on investment

-----000 -----

b) 50 million €1 micro-robberies

a) €50 million bank robbery

- Complex organisation Many people, inside knowledge, where, when, what resources, from where obtained?
- Very risky, leaky intelligence, getting caught is inevitable, could go wrong – high risk & low return on investment



- b) 50 million €1 micro-robberies
- Much less complex Needs one person, a networked computer, specialist malware (trojan/ SQL) + many good ideas – low risk / very high return on investment

BUT how do we make sense of different accounts of what cybercrime is/ what cybercrimes are?

- There exist conflicting accounts of cybercrime:
- A) In terms of their level of prevalence
- >1.5m-3m threats in 2008 alone (Symantec/Sophos) YET only
- >200 prosecutions under Computer Misuse Laws in 20 years.
- B) In terms what they are i) hacking, DDOS ii) frauds, scams iii) pornography, hate speech ??
- C) In terms the level of activity they take place at: personal, corporate, national/ international security concerns
- We tend to <u>over-problematise</u> the internet and <u>mis-understand the problem</u>. How do we make sense of different accounts of cybercrime?

Making sense of different accounts of

- "Everyone agrees that cybercrimes exist but they do not all agree on what they are!"
- Cybercrimes, like cyberspace, are informational, networked and globalized
- Cybercrimes make sense if we view them as mediated by <u>networked computers</u> and not just computers.
- We can understand cybercrimes more clearly if we apply an <u>elimination test</u> - e.g., just think about what is left after the Internet has been removed from the equation.

Evolutionary/ Generational differences in level of mediation by technology

- Traditional crime (initially mainframes 1st generation) cybercrime within discrete computing systems b) to assist traditional crime information, communications
- Hybrid cybercrime (dial-in modems 2nd generation) across networked computing systems (hacking across networks) - new opportunities for traditional crimes
- True cybercrime (Sui Generis) (broadband 3rd gen.) new forms of harm - Spams, Piracy, Phishing, making Botnets
- True Cybercrimes are networked, distributed, and automated (spam driven cybercrime – 'phishing') moving towards complete mediation by networked technologies (eg., 'phishing' into 'pharming'). (See further Wall, 2007)

Accounting for different types of cybercrime

Three generic groups of cybercrime (Wall, 2007)

- Integrity related cybercrime Hacking and cracking, DDOS
- Computer assisted cybercrime Virtual bank robbery: Exploiting financial and billing systems online
- Content related cybercrime Online obscenity (extreme pornography), violent or harmful content, Offensive communications, email, chatrooms/ blogging

These three groups are unlikely to change – just the content **BUT THE MEANS OF VICTIMISATION WILL CHANGE**.

PART 2 What recent cybercrime developments are challenging criminal justice systems

New (financial) crime motivations – increase in proportion to the amount of money available. Has been a rapid increase in volume of personal and commercial financial internet traffic. Drives the third generation of criminal activity mentioned earlier.

New forms of organisation of crime online

Sophisticated 'Crimeware as a service' being offered to create and deliver malicious software.

> Email attachments are still prevalent but more dangerous.

Use of toxic websites to launch drive-by downloads (malicious software) directly into browsers (exploiting flaws).

SEE FOLLOWING EXAMPLES - a) Crime Organisation online b) toxic www sites/ evolution of phishing

EXAMPLE ai) KNOWN 'BRANDED' ORGANISED CRIME GANGS

Superzonda – spammers - based in South America, specialize in creating and disseminating spam.

- **The Hangup Team** (red-and-black swastika shooting out lightning bolts) a Russian gang that 'SecureWorks' claims develops malware for sale to hackers. The group is believed to be still in operation creating malware. Use Coreflood and the Trojan Backdoor.Win32.Padodor.w to develop botnets. (three folk from Russia. Arrested 2000. Back in action with links to the spamming industry which uses their botnets as spamming platforms.
- Shadowcrew (Operation Firewall 2004/5) the ShadowCrew, a gang dedicated to identity theft, bank account pillage, and the fencing stolen goods on the WWW. Did not meet. No need. Surveilled online.

The Rock Phish gang – a most notorious phishing gang – reinvented itself

Drink or Die – distributes Warez – Claimed no profit .. but highly organized and security-conscious. Cracked new software and released it

Carder Planet and Darkprofits - facility for selling credit card details

Rustock, Warezov, Blackcarder, Storm Worm Gang, Celebrity Spam Gang – all control botnets

The Russian Business Network – drive-by downloads

EXAMPLE aii) What do we know about cybercrime gangs? - analysis of known gangs

They are mainly ephemeral – project based

They are self-contained - more like cottage industries

➢ Just because they are Russian or Eastern European in origin or are based upon servers is not evidence of links to traditional organised crime – which is a big concern

The new technologies are cheap and only require knowledge to implement and use – little start up cost

They do not carry the hallmarks of traditional organised crime but ... a) criminal wealth accumulates b) aspects can be useful to OC

EXAMPLE aiii) Pay per infection models – to create botnets

LAST NEWS :

Home

ac

2007-04-21 20:05:33 ВНИМАНИЕ!!!

www.iframebiz.com

2007-04-16 22:36:32 Все выплаты будут в usd!!!

2007-02-14 19:38:39 We have new EXE's please take new one Please take new EXE, for better ratio.

2007-02-13 05:53:27 Please read this!!! We need only clean installs, we don't accept installs with any other stuff.

- We give our code to your and you need to setup it to your websites. We pay for installs and for trusted webmasters for traffic if they want that.
- Average percents of loads 30-45 sometiems 48% (it's really;). It is over 10 euros for 1k traffic, our tests showed over 10Euros for 1k traffic.

Sign Up

Member

- Minimal payout summ 50Euros. By wire 100Euros
- We pay in Epassporte, Fethard, E-gold, Western Union, and other payment systems.
- We pay in euros.

Terms

- · We reserve the right to change the payment rate
- · Upon 7 days notice, we can change any terms and conditions

Rates

 Our program (size: 3 Kb) is loaded to the user and it changes the homepage and installs toolbar and dialer. It's activated and revealed in 15-30 minutes after download

- We accept any traffic !!!
- · Your account will not be deleted if you know and observe our rules.
- · You can load our soft with any metod.

EXAMPLE aiii) Pay

accept installs with any other stuff.



Example b The evolution of Identity Theft

The object of Phishing is to get victims to log onto fake www site or ring fake bank number to give personal financial information than can be used to defraud them later.

- **Trashing** (raiding rubbish bins for personal documents)
- >Phishing (sending fake bank emails asking for information)
- **SMiShing** (Phishing using SMS texting)
- **Vishing** (Phishing using VOIP)

Pharming (automatic switch to fake bank www site)

Spear-Phishing /Super-spoofing – (May2008+) adds to original screen to siphon additional information SEE NEXT - Makes fraud very personal again – account take over a) How are reputations restored b) is sleeper fraud a problem?



Dear HSBC Customer,

Your Internet Banking security code was entered incorrectly more than 3 times.

For the protection of your account we have suspended access to it.

To restore access please <u>Log In</u> correctly.

Previous notifications have been sent.

Thank you for choosing HSBC Bank. Copyright HSBC INC 2008. All rights reserved.

Example bii - Spe	ear Phishin	g – from slide by Finjan
⊖ ⊖ ▼ I ttps://bank.bardays.co.uk/olb/f/LoginMember.do	Live Search	
Efe Edit View Favorites Iools Help	🛐 + 🔊 - 🖶 + 📄 Bage + 🎯 Tgols - 👌	UNIVERSITY OF LEEDS
I BARCLAYS	<u> </u>	
Simply follow the types 1 of 2 Your Details Security Check Log_oin Step 1 of 2 Log_out the PINsentry device to hand? Just follow the Yorgotten vp PINsentry advice to hand? Forgotten vp PINsentry follow the Yorgotten vp PINsentry advice to hand? Forgotten vp PINsentry follow the Yorgotten vp PINsentry advice to hand? Select this box and then the green 'next' button to continue. Felect the green 'next' button to continue.	nu don't ur grated Help ? f? Help ? and Next }	
one IIII	v 👔 💽 Internet	

Viewed on a clean PC

Example bii - Spear Phishing – from slide by Finjan									
Our day of online of Our days.co.uk/olb/f/LoginMember.do	🗾 🔒 🍫 🗙 Live Search	🔎 🗸 🖉 Barclays Or	line Banking - Log-in Step 1 (of 2 - Microsoft Internet Explorer					
Elle Edit View Favorites Iools Help		Eile Edit Viev	v Favorites <u>T</u> ools <u>H</u> elp		A.				
😭 🏟 🚭 Bardays Online Banking - Log-in Step 1 of 2	🟠 🔹 🗟 🔹 🔂 Bage 🔹 🤅	⊚ T <u>o</u> ols → 👋 🊱 Back 🔹 (🔊 - 💌 😰 🏠 🔎 se	earch 👷 Favorites 🤣 😥 - 🖕 🚍 🦓					
M BARCLAYS		Address 🛃 http:	s://ibank.barclays.co.uk/olb/f/LoginM	tember.do	🔽 🄁 Go 🛛 Links 🎽				
		🗰 BA	RCLAYS		1				
steps 1-2 Log-in Step 1 of 2									
1 Your Details 2 Security Check 2 Security Check	?		Simply follow the steps 1–2	Log-in Step 1 of 2					
 but you know your PINsentry davide to hand? Just follow the PINsentry card reader link below to find out how. M on 9 September 2008. 	forgotten your forgotten your lessage last updated		1 Your Details 2 Security Check	Logging in with PINsentry?					
Your Details				Die you know vaa voo dan sou aan doch no on onnie banking even in you oon o have your PINsentry device to hand? Just follow het "forgotten your PINsentry card reader' link below to find out how. Message last updated oo 9. Sentember 2008.					
Please enter your membership details below	_								
Surname	Help ?			Your Details					
Membership number	Help ?			Please enter your membership details below					
Forgotten your log-in details?				Surname Help ?					
Personal/Premier customers: forgotten your PINsentr	ry card reader?			Membership number					
Business customers: forgotten your PINsentry card re	eader?			Memorable word					
Select this box and then the green 'next' butt your membership number and surname on this	computer. Help ?			First name					
If you haven't already registered for Online Banking, enjoy the benefits.	register now and			Date Of Birth(e.g. 25.05.1966)					
Select the green 'next' button to continue.				16 Digit Card Number					
	Next			Telephone banking password					
				Help ?					
		_		Forgotten your log-in details?					
Done	👔 🚱 Internet 🔍	100% -		Personal/Premier customers: forgotten your PINsentry card reader?					
				Business customers: forgotten your PINsentry card reader?					
		E Done			📋 🥝 Internet				

Viewed on a clean PC

Viewed on an infected PC



Viewed on a clean PC

Viewed on an infected PC

ਡਾ⊙ਾ ▼	🔟 🏥 🦘 🗙 Live Search	Ele Edit View Favorites Tools Help	
	🟠 • 🔝 - 🖶 • 📴 <u>P</u> age • 🍥 T <u>o</u> ols • 🐣	😋 Back • 🕥 • 💌 😰 🏠 🔎 Search 🤺 Favorites 🔣 🔗 🌺 🚍 🦓	
I BARCLAYS	*	Address 🗟 https://benk.bardays.co.uk/ob/fil.oginMember.do	V 🄁 Go Links
Simply follow the steps 1-2 Log-in Step 1 of 2		simply follow the Log-in Step 1 of 2	
2 Security Check Did you know that you can still log-in to Online Banking even if have your PINsentry device to hand? Just follow the 'forgotten y PINsentry card' reader' link below to find out how. Message last on 9 September 2008.	our don't our updated Barclays Online	Banking - Log-in Step 1 of 2 - Microsoft Internet Explorer	
Your Details	File Edit View Fi	avorites Tools Help ated	
Please enter your membership details below Surname Membership europer	Help 2 Help 2 Help 2	🔹 😰 🏠 🔎 Search 🤺 Favorites 🚱 🔗 - 🌺	
Forgotten your log-in details?	Address 🙆 https://iba	nk.barclays.co.uk/olb/f/LoginMember.do	
Personal/Premier customers: forgotten your PINsentry card read Business customers: forgotten your PINsentry card reader?	<u>er?</u>		
Select this box and then the green 'next' button to save your membership number and surname on this computer.	Help ?	CLAYS	
If you haven't already registered for Online Banking, <u>register nov</u> enjoy the benefits.	<u>v</u> and		
Select the green 'next' button to continue.	Next >	16 Digit Card Number	
		Foraotten your log-in details?	
* Your Details			
Please enter your membership details below			ernet
Surname			
Membership number			
Memorable word		Additional Fielde	
First name			
Date Of Birth(e.g. 25.05.1056)		injected by Trojan	
Date of Dira(e.g. 20.00.1900)			
16 Digit Card Number			
Telephone banking password			

Example biv - Phishing Has Evolved

- The Trojan infects and then waits for the victim to visit his or her bank – uses code obfuscation to get through AV software
- Information is gathered by injecting additional fields into the genuine bank web page as it loads in the browser
- No fake web sites changes the way bank site is viewed
- The SSL connection between client and bank is valid (padlock is shown and certificate chain is OK)
- Anti-virus software did not detect this threat
- Organisations that fail to evolve risk becoming victims of information theft
- This evolutionary force will continue a) with new technology
 b) offender need to use new tactics to trick victims

PART 3 What developments in networked

>New convergences of technology will continually create new opportunities for crime

- the inventors of the computer and telephone did not forsee their convergence as the internet! Nor of criminal opportunities arising
- Neither did inventors of phones and cameras!
- Ambient technologies via new generations of RFIDs may spawn the fourth generation of cybercrimes.

Criminal motivations will rise along with the stakes

> see the case of the magic swords (valuable intellectual properties created online).

>New forms of crime organisation online will prevail. But ...

- They will be organised more along the pro-sumption (participatory consumption) model.
- Interestingly, they are anti 'command and control'/mafia in that a) they do not require massive start up costs b) they can operate independently/ secretly c) they don't need protection

PART 4 How do we regulate Cybercrimes?

 \succ The same technologies that cause the crimes also can be used to police and prevent them.

➢We need to clarify the relationship between Law and Technology - once law becomes embedded in code it can lead to ubiquitous law enforcement ("aware of everything but itself and its own blind spots and biases" Adorno)

Primary legislation could contain rules for establishing principles and standards for technological interventions.

➢We need to be careful of a shift from a justice society to a control society where justice is replaced by risk assessment of potential criminalty based upon simulations of crime.

We need to establish a common framework of accountability that accommodates conflicting Public v Private interests





Wall, D.S. (2007) *Cybercrimes: The transformation of crime in the information age*, Cambridge: Polity. ISBN 0745627358.