


xri
xiphos research labs

Into the Black: DPRK Exploration
(Or How I Learned to Stop Worrying and Love the Bomb)



Michael Kemp
Co-Founder: Xiphos Research Labs

SECURATOR

North Korea scares people. Allegedly DPRK has a super 133t squad of killer hacker ninjas that regularly engage in hit and run hacks against the Defense department, South Korea, or anyone else who pisses off the Dear Leader. DPRK also has no real Internet infrastructure to speak of (as dictators don't like unrestricted information), although it does have a number of IP blocks (unused?). This talk examines some of the myths about DPRK, and some of their existing and emerging technologies. In 2008, Orascom Telecom formed a partnership with the DPRK government and set up the state run mobile carrier, Koryolink, and DHL are part of the European Business Association (presumably for when dictators need to "Add Value, Be Valued"). This talk examines some of the available infrastructure associated with DPRK (funnily enough some of which is in South Korea and Japan) and explores the potential technical threats posed by a pernicious regime, as well as exposing some of the huge gaps in logic that have led to the world potentially engaging in chicken little syndrome when it comes to DPRK. No 0days will be demonstrated, however this talk will discuss some new information that hasn't yet been made public.



Standard Disclaimer

The views, opinions and details presented in this resource are solely those of the author, and not of any present or previous employer or organisation. No warranty is inferred or granted. Additionally if I am black bagged, please contact North Korea and see if you can find me (although to be fair they largely stopped that in the eighties)

"If there was hope, it must lie in the proles, because only there, in those swarming disregarded masses, eighty-five percent of the population of Oceania, could the force to destroy the Party ever be generated."

George Orwell, '1984'

"I am an Internet master"

Kim Jong Il, 2007



Who am I?

UK based security consultant, application vandal and general trouble causer

Co-Founder of XRL (UK/US based security consulting and software house)

International Speaker

Am not now, nor have ever been a member of the Communist party

Am not now, nor have ever been an Intelligence Operative

Have not been to DPRK, and don't speak Korean, so my pronunciation will be all kinds of wrong

Am sick of the whole "cyber" warfare sideshow



Fear
Black holes
Super hackers
In & Out Relationships
Apologies

What's this talk about?

Everyone it seems is scared of North Korea (DPRK)

It's part of the Axis of Evil (which makes it sound like it belongs in a Batman comic)

DPRK is a Stalinist dictatorship ruled by an iron cult of personality

Apparently they have evil super haxors

It's also an Internet black hole

Examination of external security and internal infrastructure (and the weird international relationships)

Might not seem to be about "hacking"... It is though... Kind of...



Oday

Tech demo

Vendor Pitch

Fear & Loathing



What's this talk isn't about?

No Oday

No tech demo

No vendor pitch

No unjustified chest beating

No ego



When most people think of the Democratic Peoples Republic of Korea (North Korea) there are a few things that come to mind...
There's more to DPRK than this...



Since I gave this talk @ CONFidence in May, North Korea is in the news again...

North Korea suddenly remembered in was 'officially' at war with the South in March 2010, when the SK battleship, Cheonan was sunk

The South Koreans quickly unearthed a torpedo, the North quickly said it was a US mine that led to the ship being sunk...

Whatever the situation, 46 people are now dead, and this talk may have increased in topicality. The former sucks...

Image Source: http://www.wired.com/magazine/2010/05/st_manganews



Part the First

*Wherein an attempt is made to distil the
infrastructure technology and relationships of a
nation state into thirty slides*



Part the First

Wherein an attempt is made to distil the infrastructure technology and relationships of a nation state into thirty slides

“Citizens are guaranteed freedom of speech, of the press, of assembly, demonstration and association.

The State shall guarantee conditions for the free activity of democratic political parties and social organizations.”

Article 67, DPRK Socialist Constitution

Source: http://www1.korea-np.co.jp/pk/061st_issue/98091708.htm



Limited, Restrictive and Expensive

Intranet (Kwangmyong) not Internet

KCC – 2003

What's going on?



DPRK has limited Internet access

It does have Intranet access (highly restricted and very expensive)

The DPRK Intranet was set up in 2000, however was expanded by the KCC (Korea Computer Center; about more later) branch in Berlin in 2003

The branch helped refine the Kwangmyong Intranet (at a reported cost of \$950,000)

So, what is Kwangmyong and how does it work?



"...all other people use Kwangmyong"

Kwangmyong ("Bright") is the DPRK approved version (e.g. Intranet) of the Internet. The unrestricted Internet can only be accessed by approved officials (how?) and according to Wikipedia, "...all other people use Kwangmyong. This is a free service for public use."

I would argue that not everyone can use Kwangmyong as hardware costs are restrictive in an economy where the average income is believed to be less than \$1900 per annum (Source: CIA World Factbook)

Ignoring Wikipedia's rose tinted view however...



In 2001, the Shengyang China based financial institution, Silibank offered email relay services for DPRK.

As of 2007, Silibank was now longer online...

Kwangmyong is the ultimate walled garden...



For internal use, Kwangmyong was launched in 2000, and is reported to consist of a browser, email program, filtered news groups, and a heavily filtered search engine. For a resource to make it onto Kwangmyong it first has to make it past the regimes' censors.

The Kwangmyong Intranet can be accessed via dial up with servers located in China. Kwangmyong is the ultimate walled garden...

Five landlines to every One Hundred people



Apart from Kwangmyong, how else can the 'hermit kingdom' communicate?

DPRK is still resilient to the telephone

According to Marcus Nolan & others, there are only 1.1 million landlines in DPRK (or 5 landlines to every 100 people)

Plans were afoot to expand this in 2003, but in 2007 DPRK again restricted telecoms use



Automated switching is reportedly in use around the capital, Pyongyang, however much of the infrastructure controlled by the North Korea Post and Telecommunications system is reliant on manual switches

The automated switches in use on the telephone backbone are provided by Alcatel Shanghai Bell (<http://www.alcatel-sbell.com.cn/>)

Making and receiving phone calls outside of Pyongyang is problematic, and hand cranked phones are still in use widely

I'll discuss telecoms in more detail later...



Aside from Kwangmyong, it is possible for an elect elite to access the Internet (kind of)

In 2005, RENK published details of an Internet cafe in Chongjin, known as the "Information Technology Store"

Image source: <http://www.dailynk.com/english/read.php?catald=nk00300&num=206>



The Information Technology Store is one a very few state sanctioned Internet cafes (only two widely known)

It was opened in 2005, and according to available reports charges customers 20,000 won per month

The average monthly salary is 3000 won

In 2002, Kim Beom Hoon (Hoonnet.com) established a gambling site with the help of the DPRK government investment, and opened an Internet cafe in Pyongyang ("Internet PC Room") which charged \$10 per hour

\$10 is about 1500 won (estimates vary but \$1 averages at about 150 won) – or about two weeks salary – Before closure this cafe was believed to be restricted to foreigners
According to the AFP News Agency and Reuters, 2007 saw a backlash against Internet cafes, and they were closed



Nobody really seems to know for certain how North Koreans connect to the Internet, but the reality is that very few do, and those that do, are highly and tightly regulated (apart from the upper party echelons)

Apart from dial up connection to Chinese ISPs the Internet in DPRK can also be accessed via satellite

Another mechanism for accessing Kwangmyong is allegedly via servers located in Germany and controlled by Jan Holtermann (about more later)

Satellite connections are apparently in use in a number of 'tourist-friendly' hotels in Pyongyang, however there use is not widespread (factors of cost, and access to tech play a part as well as state control)

Nobody really seems to know for certain how North Koreans connect to the Internet, but the reality is that very few do, and those that do, are highly and tightly regulated (apart from the upper party echelons)



In 1986, DPRK (and France) established INTELSAT satellites above the Indian Ocean allowing for 35 FDM (Frequency Division Multiplexing – e.g. Different frequency band for each signal simultaneously transmitted on single carrier) and 18 SCPC (Single Channel Per Carrier) connections allowing both television and satellite communications

In 2001, DPRK joined INTELSTAT (International Satellite Telecoms provider) and relies on satellite networks to connect to Japan and the United States

In March 2009, DPRK claimed to have launched its own orbiting satellite (the Kwangmyŏngsŏng “Bright Star” experimental satellite program has been allegedly operating since the 1980s)

According to US, Russian, and South Korean officials, however both the 2009 rocket and the satellite payload ended up in the Pacific Ocean



1990 – 3 Direct Lines to Japan

1995 – Direct line to USA (courtesy AT&T)

2000 – 29 direct lines to South Korea
(total of 56 via 3rd country relays)

2008 – Majority of IDD connections
disabled

In 1990, agreement was reached between Japan and DPRK to allow for 3 phone lines (as well as INTELSAT)

In 1995, AT&T agreed a direct link between DPRK and the US (they'll censor 4chan but not dictators)

Communications between South and North Korea were opened in 2000 with 56 lines (29 direct, mostly for ministerial talks, and the rest via third country relay networks)

International connections beyond state control (e.g. through relays) are a concern to DPRK

An unauthorised phone call to China can result in a heavy fine – a call to South Korea, imprisonment (or worse) – As part of this research I thought of wardialling DPRK but realised it may do more harm than good

In 2008, DPRK reportedly disabled the majority of the IDD connections it has

DPRK International Operator = +850 2 18111

192 + 7 digit - Koryolink 3G Network (about more later)

193 + 7 digit - SunNet GSM/900 Network

Known DPRK City Codes

2 - Pyongyang
31 - Moranbong
39 - Nampho
41 - Songnim
43 - Songnim
45 - Haeju
53 - Hungnam
57 - Wonsan
73 - Chongjin
85 - Rason



The majority of phone lines in DPRK can only be called from outside the country only through the operator service.

Several "approved" subscribers have the "privilege" of the possibility of being called by direct dialling (it is not known who, and I wasn't about to find out).

According to Ken Westmoreland & World Telephone Numbering Guide (<http://www.wtng.info>):

"There are two number ranges in Pyongyang:

Numbers beginning with 381 are for international inbound dialling only, while those beginning with 382 are for domestic dialling only. It is not possible to dial a 381 number from a 382 number, or vice-versa. Hence the British Embassy's telephone number within North Korea is (02) 382 7980, while from outside the country, the number is +850 2 381 7980."



koryolink - Democratic People's Republic of Korea



Financial Data

Operational Data

	December 2009	December 2008	YoY (%)
Revenue (USD 000)*	-	25,891	N/A
EBITDA (USD 000)*	-	17,133	N/A
EBITDA Margin	N/A	66.1%	N/A
Capex (USD m)*	N/A	27	N/A

	December 2009	September 2009	December 2008	YoY (%) Dec. 2009 vs Dec. 2008
Subscribers	1,864	69,281	61,754	N/A
Market Share (ARPU (USD)* (3 months))	100.0%	100.0%	100.0%	0%
Avg MOU (YTD)	N/A	319	239	N/A



In 2008, the Egyptian company, Orascom were awarded a contract to provide a GSM network to DPRK (only covers Pyongyang)

Claiming over 90,000 subscribers as of 2009 (how given the cost of mobiles???)

25% of Koryolink is owned by Korea Post & Telecommunications Trading Corporation

Subscribers can access the Kwangmyong portal via mobile 'browsing'

Can't find many details on Koryolink and how it works... Apparently if you want to dial a subscriber (don't!) it's similar to the now banned SunNET network (e.g. 193 801 plus 4 digit subscriber number)

As to the network backbone – I have *no* idea....



DPRK is not without technical institutions – the most famous of which is the Korean Computer Center in Pyongyang

Founded in 1990, the KCC has in recent years been supplemented by branch offices in Germany (headed by Jan Holtermann), UAE, China and Syria

Publicly a research institute, the KCC has developed a range of software that is known about publicly...

It also has a number of companies trading from its premises...

Also there is the Pyongyang Informatics Center (established 1986) which has much the same remit...



The KCC has produced a number of 'public' software apps:
The search engine component for Kwangmyong "sam heug".
Korea writing program "The Naenara"
Korea game play program "The Chosun Jang-Gi"
Korea national program "The GwanMyong"
Korea food study program "The Chosun Ryo-Li"
"Koryo", English-Korean/Korean-English translation software using an electronic pen
Korean language Voice Recognition Software "Nunbora"
"Cyber Friend", Video Conference System
"Cyber Star", Distance Education System
Computer Go Software "SilverStar Paduk"

& a Linux Distribution (Korean Edition) called "Pulgunbyol" (also known as Red Star)



In February this year, a Russian blogger ashan_rus, published detail of Red Star.

Apparently it was created at the behest of Kim Jong Il and included in the read me is the quote "You must create a system based on the Linux kernel in our [Korean] style."

It's not finalised or stable yet... (just like any other distro)

Apparently Red Star costs about \$5 in Pyongyang markets... It's not entirely clear how ashan got his copy (although he is a student at Kim Il Sung university).... And indeed what the OS actually does (with regards monitoring)

An OS is all well and good but given hardware costs who can actually use it??



As well as producing software the KCC also hosts a number of DPRK / foreign companies....

Nosotek was set up in 2008 to provide out-source software development in DPRK (not that I'd trust DPRK dev work not to be shady...)

Founded by Volker Eloesser (ex-Verisign and ex-lecturer at the Pyongyang Business School) one of their major 'advantages' is "Low-cost HR" (or slavery even...)

Into the Black: DPRK Exploration / Inside Out

xri
alpha research lab



NOSOTEK.
IT-Outsourcing redefined

KCC
KOREA
COMPUTER CENTER

BIRINDELLI
& ASSOCIATI

K-P
Korean-Polish
Shipping Co. Ltd.

RUSSIAN RAILWAYS
Joint Stock Company

DHL

dat activity
The Human Touch
in Data Processing

orange

BT

Tel: +44(0) 208 992 4965.
E-mail: singuk.ha@btinternet.com

SECURATOR

Nosotek aren't alone....

The Swiss based Data Activity outsource data processing to DPRK... The Italian law firm Birindelli & Associati has an office in Pyongyang... There is a Korean-Polish joint venture (the Korean-Polish Shipping Co Ltd).... Even DHL have office in Pyongyang

Talking of Poland... Poland still (even though it is no longer a "friend" state) exports to the DPRK and provides grants (which may or may not be used for medicine and farming equipments)

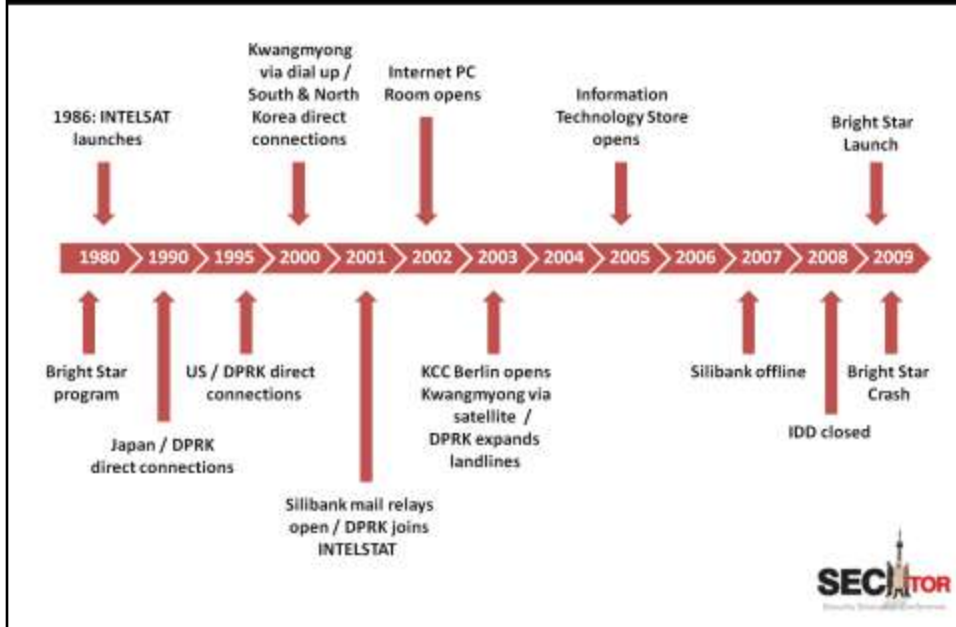
British Telecom provide the email address of the DPRK ambassador in the UK (in France it's Wanadoo/Orange)

If DPRK is such an evil system, how are so many companies supporting it??



DPRK embassy in London is in a suburb called Ealing...

Into the Black: DPRK Exploration / Inside Out





Part the Second

*Wherein myths are debunked and questionable
research results presented for purposes of
edification and entertainment*



Part the Second

Wherein myths are debunked and questionable research results presented for purposes of edification and entertainment

The Mystery of Unit 121



In May 2009, Major Steve Sin (US Army) published the paper 'Cyber Threat posed by North Korea and China to South Korea and US Forces Korea'

In it he outlines Unit 121, a supposedly elite unit of DPRK forces dedicated to cyberwarfare activities

The source of this data is the Yonhap News Agency (who interviewed an 'anonymous' source). The YNA is funded by the South Korean government

Also cited was an article entitled 'Inside DPRK's Unit 121' written by Kevin Coleman and published by DefenseTech in 2007



X 17,000



Unit 121 supposedly consists of up 17,000 personnel (that's a lot of uber haxors) situated in the KCC in Pyongyang

They apparently possess 'Moderately advanced distributed denial of service (DDoS) capabilities with moderate virus and malicious code capabilities'.

They are also apparently responsible for attacking the West, and generally being willing technical ninjas for Kim Jong Il

Sadly, apart from the not particularly independent sources, I could find no other credible mention of the very scary Unit 121, so I got in touch with Kevin Coleman...

Dear Mr Coleman,

I am currently seeking to obtain further details regarding a military unit as mentioned in your piece, <http://defensetech.org/2007/12/24/inside-dprk-unit-121/> (published December 2007). As part of the preparatory work involved in preparing a presentation to be delivered at a number of international IT security conferences, I am currently engaged in research concerning the offensive capabilities of DPRK particular with reference to information warfare.

The article published in December 2007 alludes to a seemingly unsubstantiated military unit with such capabilities (an attributable, named source seems somewhat hard to come by). I would be interested to know how such data was collated and sourced. The only sourcing I can find appears to be from the Yonhap News Agency (as funded by the South Korean government) or from an 'anonymous' source. Bearing in mind the arguable non-impartiality of the first agency, and the lack of journalistic best practice is quoting the second, I would like to enquire as to the source (if differing) of the material, and the journalistic accuracy of the assertions made in the article.

To Me:

A couple of things

1. The tone of your email puts me off as well as our ops team that responded to your email to info@technolytics.com. They called me!
2. Google North Korea Unit 121
3. Look at the attribution of the July 4th cyber attacks on the U.S. South Korea and the US both point back to North Korea.

Other than that I am not inclined to issue any further data given you tone/attitude and the fact that most of our work is classified and not available for public disclosure.

To Me:

I suggest you contact your MI5 and Major Sin if you would like to substantiate N Korea's cyber capabilities or look at the attribution to the July 4th 2009 events

To Me:

Well there are those that think the unit number is 110 or 101 you might want to check that as well.

To Me:

You clearly have an agenda and I am through wasting my time.

To Kevin:

The feeling is mutual I assure you. As for my agenda, if you call asking for attribution from a journalist whose 'evidence' is being utilised to shape public opinion, government policy, and doubtless company profit margin an agenda then, yes I do. It's called seeking to ascertain the truth (perhaps an oddity given the preponderance of unnamed and unnamable sources when 'reporting' on information warfare). As you seem unwilling, or unable to substantiate your claims, I'll treat them with the seriousness that they doubtless deserve.

That said, many thanks for your time, and considered responses.

The Point:

Apparently the only sources for Unit 121 are 'classified' or otherwise obfuscated

Presented as fact

Kevin Coleman is associated with Technolytics which provide cyber war training and advice

He also came up with the definition of cyber-terrorism (according to wikipedia)

He also presents to US congress

He can't source his allegations publicly....

Errr.....



Just to clarify; I am willing to publicly admit I am completely wrong and offer a full apology if I can get attributable independent sources....

The point was not to attack a particular 'expert' but rather suggest that proof is kind of useful....

Until proof is shared I call FUD and BS

Incidentally the mail chain between Kevin Coleman and myself is available if anyone wants it...



Kevin Coleman
Worlds No. 1 Cyberwar Expert?



Gregory Evans
Worlds No. 1 Hacker?





“Cyberspace has become the fifth domain of warfare, after land, sea, air and space”

“A lot could be achieved by greater co-operation between governments and the private sector”

“One response to the growing threat has been military. Iran claims to have the world’s second-largest cyber-army. Russia, Israel and North Korea boast efforts of their own”



July 2010 – Economist (2 articles / Leader column on Cyberwar, and Cyberwar: War in the fifth dimension”

Quote 1 = Has it? Er... When?

Quote 2 = Sounds a tad worrying. What wonderful Orwellian powers are being suggested. The second article makes frequent reference to “cyber-weapons” and their ease of creation....

Quote 3 = Questions of attribution (again)... I sent them an email...

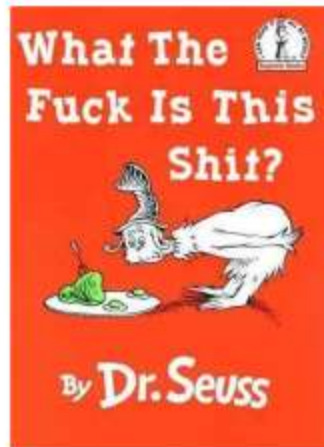
Read the article without paying the Economist:

http://www.economist.com/node/16481504?story_id=16481504

To: Economist PR (as they don't have an editorial contact, and both Cyberwar articles are written by un-named 'journalists'):

I am writing to you with regards the Cyberwar / Leaders piece recently published in your July 2010 edition of The Economist. For the last eighteen months I have been studying the technical capabilities present in North Korea, and the digital threat that they pose...In all my research thus far, I have not been able to source a single substantive claim regarding the information warfare capabilities of North Korea...

Given that in my research thus far, I have found no mention regarding the information warfare capabilities of North Korea from any source other than anonymous sources, or from organisations with a vested interest in claiming as much (e.g. organisations that provide information warfare training), I would be very eager to discuss the source for the claim made in this piece.



- 1 – State something nobody can prove or disprove
- 2 – Watch it make press
- 3 – Reinforce claims
- 4 – Watch it make more press
- 5 – Panic spreads, so does spending
- 6 – ???
- 7 – Profit?

Vested interest may have invented unsubstantiated rumours of DPRK ninja hit squads. Rumour is reinforced by it being quoted (Steve Sin). Rumour is picked up as fact (Fox News). Rumour proves useful (South Korea). Rumour gets picked up by thought leaders / credible press (Economist / Pearson International). Politicians and defence invest in vested interests



Seriously just because Pearson / The Economist doesn't believe in having attributable, named, journalists – they should at least do some fact checking no?

The warning labels are from <http://www.tomscott.com/warnings/> - he even does them in Swedish



Defcon 18

August 2010

Kim Jong Il & Me: How to build a cyber
Army to attack the US

Charlie Miller



Earlier this year, Charlie Miller gave a talk at Defcon 18 in Las Vegas

For those of you who don't know who Charlie is (cave dwellers) he used to work for the NSA, won the CanSecWest PwntoOwn in 2008 with Android and iPhone 0day and is a definite "name" in security

An amazing researcher. I am sceptical of anyone who has worked for government. I am equally sceptical when someone goes from doing practical goal focused research to making proclamations about North Korea and cyberwar

I am now about to pick a fight with one of the worlds best researchers and an ex-spook (I've already pissed off DPRK after all), but I'll try to be nice...



Juche is the ideology that lies at the heart of North Korea.

Originally conceived by Kim Il Sung, it holds that “man is the master of everything and decides everything” (sorry ladies)

Basically, it's isolationist in tone, and one of its central premises is that North Korea should provide for itself (hence the development of North Korea software and space hardware)

Consists of three key elements; "independence in politics" (*chaju*), "self-sustenance in the economy" (*charip*), "self-defence in national defence" (*chawi*)

Juche is incorporated not only in state ideology but also military policy – The latter is worth remembering...



Charlie begins his talk by outlining North Korea military spending. He puts the figure at \$5 billion. According to Charlie, the US spends \$703 billion

According to the Stockholm International Peace Research Institute (SIPRI), he's right...

There are voices of dissent though. According to an article published by Asia Chronicle in July 2009, John Feffer claims that for all the people in uniform DPRK only spends half a billion dollars annually on its military. John Feffer is a researcher (specialising in DPRK) at the Institute for Policy Studies (US, left leaning think-tank with Noam Chomsky as a Senior Scholar)

Regardless of military spend, Charlie outlines a scenario whereby it is possible for DPRK to win a 'cyberwar' for *only* \$49 million...



According to Charlie's plan: North Korea needs to hire sploit developers, coders, bot collectors and operators, managers, testers, sysadmins, and remote personnel (basically they need a mini version of the US Cyber Command (American tax dollars at work there...))

If they can gather those personnel, they can create Oday, herd there own (and borrowed) botnets, plant insiders at sensitive controls, and create havoc

Apparently they only need 592 people to do all this... So who knows what the 17 thousand at KCC are doing....



- 1 - DPRK does Juche
- 2 - Managing remote agents is hard
- 3 - Recruitment is a bitch
- 4 - Er, why?

There are a few problems with Charlie's scenario:

1 - It calls for the recruitment of external personnel. For political (and maybe economic grounds) this idea might not be acceptable to Kim and co

2 - The plan also calls for the insertion of personnel into 'hard' targets. This is difficult. It also calls for the management of these personnel. With DPRK's limited comms capabilities this may also prove tricky

3 - It's arguably not morality that stops people turning to the dark-side, but fear of jail and getting killed. If you are worried that Russian mobsters may kills you, DPRK almost certainly will if you screw up. The reward, a salary of 100k a year. Soooo, not worth it

4 - If North Korea went after core routers and carrier networks it would cause chaos, but why do it? There are softer targets (e.g. Hospitals), and any targets will lead to reprisals...

Unlike many Charlie however, does caveat what he is saying, "North Korea can can't t easily do this, and this attack suffers from being hard to carry out and largely unnecessary", he also states (rightly) that North Korea can function without the Internet (er, yeah as they don't technically have it)



I have a few simple conclusions about Charlie's talk....

Is it theoretically possible? Yup. It is also theoretically possible that I may stumble across a shipping container full of cash. Neither is particularly likely

The whole 'cyberwar' thing hasn't happened yet, why not? See Marcus Ranum, and common sense (e.g. If you are a small nation you are not going to start a fight with a large one that will destroy you – see Iraq)

There are enough right wing idiots with agendas (e.g. Richard.A.Clarke, ex Bush special advisor on cyber security, now chairman of Good Harbor Consulting, who do risk management and cyberwar training, which is nothing to do with his book 'Cyber War' published in April 2010) without talented researchers joining in....

The talk is good (see for yourself at <https://www.defcon.org/images/defcon-18/dc-18-presentations/Miller/DEFCON-18-Miller-Cyberwar.pdf>) but it makes massive assumptions about DPRKs infrastructure, staff management and espionage capabilities.

Could they do it? Probably.... Will they? Almost certainly not.... Nothing to see hear move along....



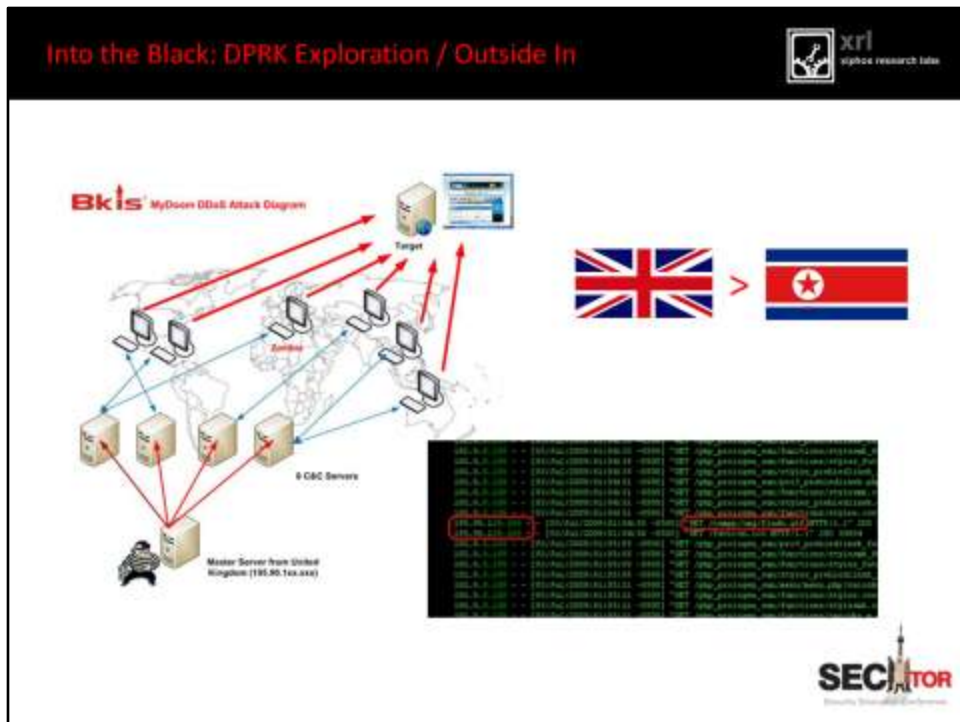
Starting July 2009 a number of DDOS attacks were enacted against targets in the US (Treasury, State Department, White House) and South Korea (25 banks)

These attacks were quickly heralded as proof of the evil and I33t DPRK hackers

The Korean CERT (KrcERT) requested Vietnamese security company, Bach Khoa Internetwork Security to investigate (<http://blog.bkis.com/en/korea-and-us-ddos-attacks-the-attacking-source-located-in-united-kingdom/>)....

Meanwhile in America... Peter Hoekstra (Republican / House Intelligence Committee) pointed squarely at North Korea and demanded a retaliatory strike stating that: "next time they'll go in and shut down a banking system ... or manipulate the electrical grid either here or in South Korea. Or they will try and miscalculate, and people will be killed."

This is the same guy that in 2006 announced that WMDs had been found in Iraq, and has been found to provide misleading evidence about Iran, so he can clearly be trusted...



BKIS were able to gain access to 2 of the 8 C&C servers, that were responsible for directing the attacks, but more importantly found an additional server located in Brighton, in the UK (belonging to Global Digital Broadcast / <http://www.globaldigitalbroadcast.com/>) - My guess as to IP would be 195.90.118.102 (whatever it was it'd dead now)...

Although master server was owned by a company in the UK, it was actually being VPNed into from a partner server owned by Digital Latin America, and located in Miami, US

Official statements from DLA have said that viruses were found on the Florida server; what they were however is not public knowledge

What is public knowledge is that the server controlling attacks against the US (and SK) was not located in DPRK but in the US.... BKIS estimate that there was 160,000 bots involved spread over 74 countries



**THESE AREN'T THE DROIDS
YOU'RE LOOKING FOR...**



The botnet was big... The malware wasn't....

Based on the MyDoom codebase (2004?) seemed to be cobbled together from scripts, made no attempt to bypass AV, and used a Korean language template

Compare this to GreyPigeon and Chinese malware, which when it first started was also cobbled together from existing available materials.... Could be a clue to origin

A hacker operating beyond the DPRK military would not be able to create this (and they surely would do a better job?). Maybe it's Chinese, maybe it's American, my guess (and the guess of Jeffrey Carr of Project Grey Goose is that the country of origin is unlikely to be North Korean. Still, the bogeyman is an easy target....



In 2004, LT. General Song Young-guen, of South Korea's Defense Security Council announced at the Defense Information Security Conference that DPRK had a highly skilled military unit intent on hacking South Korea

According to the General, they have the equivalent skills of the CIA (so better than moderate ability then?)

This has been disputed by a number of experts, most notably John Pike of Globalsecurity.org

For a while Kuji (Mathew Bevan) and Datastream Cowboy (Richard Pryce) were thought to be North Korean (because of attacks on the USAF, Lockheed)... Kuji is not from North Korea, he's from Cardiff...

According to both South Korea NIS (National Intelligence Service) and KISA (Korea Information Security Agency) there is no credible evidence for super hackers in the North....



There is something about South Korean generals....

In June 2010, Maj. Gen. Bae Deuk-sik (again of the DSC) stated that DPRK was likely to target the G20 meeting in November in Seoul ("To disturb the G-20 Summit, the North is likely to conduct a massive cyber attack, of which it is easy to destroy evidence,")

http://www.koreatimes.co.kr/www/news/nation/2010/06/113_67314.html

After what happened with Ian Tomlinson at the G20 protests in London (April 2009) I would think a lot of other people (in addition to DPRK) are pissed at the G20 too...

Guess we'll see what happens in November, but given the shocking events of 2004 (e.g. nothing) I remain sceptical...

From the Batshit Crazy Department...



May 2010 saw the news that North Korea was behind the Gulf Oil Spill

According to right wing and neo-conservative US bloggers, the DPRK sent a cargo ship staffed by a 'suicide squad' which then launched three torpedoes at the Deepwater Horizon. Another theory holds that the same suicide squad used an advanced stealth submarine...

Why? Well obviously to start a war, and because the Deepwater Horizon rig was made by South Korean manufacturer Hyundai Heavy Industries

For more silliness: <http://www.eutimes.net/2010/05/us-orders-blackout-over-north-korean-torpedoing-of-gulf-of-mexico-oil-rig/>



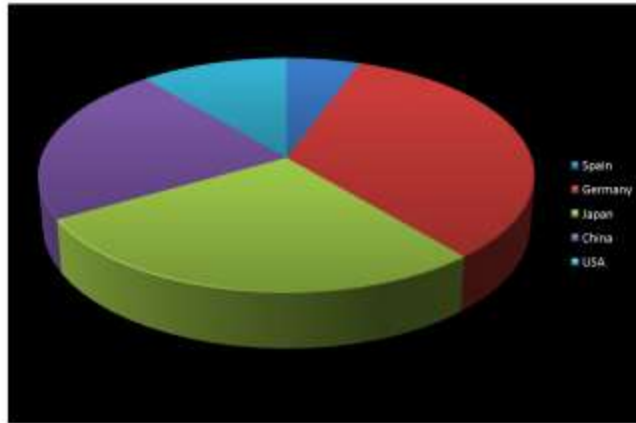
As part of preparing this talk I wanted to see what infrastructure I could find (especially as I couldn't find a way to play with Koryolink)...

As highlighted there are no direct and easily accessible links from DPRK to the rest of the world so, I looked at what was available

Researchers estimate that the number of Internet resources directly related to DPRK is about 30.... I found 18....

Wanted to (legally) examine them to see what state they were in (e.g. Do DPRK have Gold builds??)

korea-dpr.com – Official Webpage of The Democratic People’s Republic of Korea
naenara.kp – DPRK news and shopping portal
kcna.co.jp – DPRK news service in Japan
korea-np.co.jp – The Peoples’ Korea
dprkorea.com – Holding page (looks to be a trade organisation)
uriminzokkiri.com – Pro-Korean unification
aindf.dyndns.org – Anti-Imperialist National Democratic Front
alejandrocaodebenos.com – Korean Friendship Association (President)
business-school-pyongyang.org – DPRK / Pyongyang Business School
koryogroup.com – Koryo Tours / DPRK Tourism
ournation-school.com – DPRK / Juche education?
korea-publ.com – DPRK publications (Amazon for Kim Jong Il)
korea-is-one.org – Pro-unification
kdvr.de – German based, Korean pro-unification
chongryon.com – General Association of Korean residents in Japan (pro-DPRK)
juche.v.wol.ne.jp – International institute of the Juche idea
eba.nosotek.com - DPRK European Business Association
kckcp.net – Korean Computer Center



Where has the most sites associated with DPRK??

Germany = 6

Japan = 5

China = 4

USA = 2

Spain = 1



Microsoft IIS = 6

Other = 1

Apache = 11



Oldest iteration of IIS in use was 5.0

Oldest iteration of Apache was 1.3.41

Of the found hosts:

58% had FTP (TCP 21 open)

29% had SSH (TCP 22 open)

29% had SMTP (TCP 25 open)

Most of the software used was deprecated (bug laden)

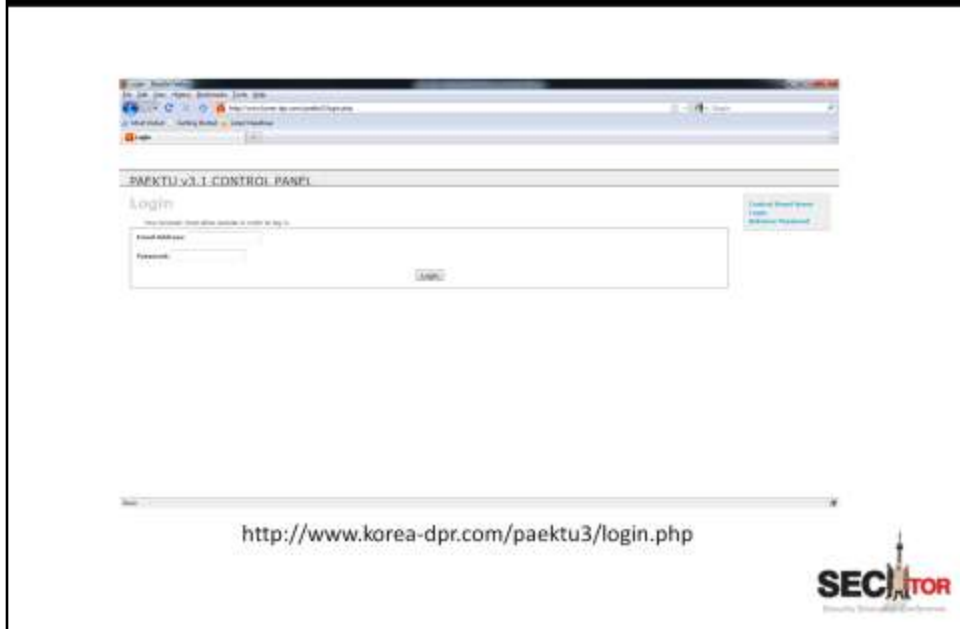
Most of the sites had HTTPS/ALT set up for auth

A couple *looked* to have trivially brute forced DB access...

Most interesting was a custom Java component on one site which I wasn't brave enough to play with...



Full system details (that I have been able to obtain legally) available upon request...



The Official DPRK site uses WordPress (see: <http://www.korea-dpr.com/forum/wp-login.com>)

More interesting is its use of Paektu (<http://www.korea-dpr.com/paektu3/login.php>)

There is no reference to Paektu anywhere that I can find. Looks like a DPRK web server / app control panel (wonder how vulnerable it is?)

The only other references to Paektu are about Kim Il Sung and Mount Paektu

Is Paektu a product of DPRK? Where else is it installed? What is it & where is it from??



Very odd North Korean kids TV and more @
<http://www.youtube.com/user/uriminzokkiri#p/u/23/aWh9RmtRIIk>

DPRK does Twitter:
<https://twitter.com/uriminzok>

Dictator Tube
Because propoganda can be fun



In 2009 North Korea started a twitter account (kcna-dprk) which was promptly suspended

In August (the 12th to be exact) the North Korean media agency (or propaganda department) Uriminzokkiri (Our Nation) opened an account @uriminzok. They also have a Youtube channel (<http://www.youtube.com/user/uriminzokkiri#p/a/f/0/ymGmMINS-Zs>)

It's not clear who is updating these resources (I'm guess Germany or a 'friend' in the West)... It's nice to see North Koreans using 'social' media - however much of a misnomer that may be...



Warning: mysql_send() supplied argument is not a valid MySQL result resource in D:\Eminozokkiri\Eminozokkiri2011\fire\give.php on line 27
Warning: mysql_fetch_array() supplied argument is not a valid MySQL result resource in D:\Eminozokkiri\Eminozokkiri2011\fire\function.php on line 1135
해당 기능이 존재하지 않습니다.

DPRK can haz MySQL



Just as an aside, I haven't had a chance to "investigate" www.uriminzokkiri.com yet... They do have a MySQL backend though....



Without performing a full (and utterly illegal) audit against DPRK affiliated sites it's impossible to tell how secure they are

They are running deprecated software, have extraneous services enabled, and look to be susceptible to a number of common attack vectors

These servers / apps are not in DPRK, but the face that is shown to the world. If DPRK are so l33t, wouldn't there public face be a bit more secure?

It could be double bluff, they could be as useless as most other countries when it comes to Internet security, they could be concentrating on other things (e.g. Domination of the Imperialists) or they could just not have the technical aptitude..... Alternatively I could be reading way too much into it...

Allegedly naenara.kp has SQLi / XSS on it (dockdel on Reddit)....

So, are we all doomed?

DPRK has a very tightly regulated use of ICT

DPRK is a poor country with an evil little shit in charge

It seems credible that the DPRK military may be thinking about information warfare (it's cheap after all)

The skills gap

Outsourcing to China or elsewhere

Instead of worrying about digital Armageddon; worry about human rights

There may be a *lot* to explore; if you feel brave ;)





Questions?

Comments?

Abuse?



References



RENK (Rescue! The North Korean People Urgent Action Network)
<http://www.bekkoame.ne.jp/ro/renk/englishhome.htm>

A Guidebook for European Investors in the DPRK
<http://www.dprkguidebook.org>

<http://www.scribd.com/doc/15078953/Cyber-Threat-Posed-by-North-Korea-and-China-to-South-Korea-and-US-Forces-Korea>

<http://defensetech.org/2007/12/24/inside-dprks-unit-121/>

<http://blog.bkis.com/en/korea-and-us-ddos-attacks-the-attacking-source-located-in-united-kingdom/>

<http://greylogic.us/>

<http://www.scribd.com/doc/24587105/The-Dark-Visitor-Scott-J-Henderson>



In preparing this presentation I called upon a number of conflicting references in terms of published hard copy materials, Internet resources, and resources from both government / military and NGOs. This is far from a formal reference list, but should enable anyone interested in the hermit kingdom with some resources to start with.

References



<http://ashen-rus.livejournal.com/4300.html>

<http://www.nosotek.com/>

<http://www.interview-blog.de/unternehmerinnen-und-geschäftsideen/interview-with-volker-eloesser-president-of-nosotek-jv-company-in-north-korea/>

<http://dataactivity.com/>

http://www.youtube.com/watch?v=_AZnlyKXGPM – video about EBA / Nosotek

Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of North Korea - <http://www.fas.org/irp/eprint/cno-dprk.pdf>

<http://www.hrw.org/asia/north-korea>

<http://www.amnesty.org/en/region/north-korea>





Work (Hire us):

www.xiphosresearch.com
mk 'at' xiphosresearch.com

Personal (Stalk me):

www.lowfisecurity.com
clappymonkey 'at' gmail.com
[Twitter.com/clappymonkey](https://twitter.com/clappymonkey)

Location (Find me):

United Kingdom / Above the earths' core



If you have any questions for me, please let me know. I'll do my best to answer them as accurately as I can.

I'd also welcome any comments regarding this presentation, either what you liked about it, or your suggestions for improving it.

If you're curious about my bile filled life, take a look at my website
<http://www.lowfisecurity.com>.

If you want to hire Xiphos Research Labs, feel free to stop by
<http://www.xiphosresearch.com>

If you want to sell me V!AgR4, you may do so at clappymonkeyatgmaildotcom

If you want to see when I last went to the toilet, you will find me at
<http://twitter.com/clappymonkey>

Thanks



The con organisers for having me
MF for putting up with late nights &
paranoid rants
All the crew @ XRL for read throughs &
suggestions
GCHQ for listening to my phone calls
All the research bodies and NGOs doing
active research into DPRK
All the cyberwar pundits for pissing me off
YOU for listening



A big thanks to all those mentioned. Standard disclaimers apply...