AVAILABLE SOON
RATIFIED BY A NATION STATE YOU LIVE IN
ENFORCED IN ALL OTHER NATIONS
YOU COULD TRY TO DO BUSINESS WITH

THE EXTINCTION OF TRUST

based on FRIEDRICH NIETZSCHE
"Convictions are more dangerous enemies of truth than lies."

Edward J. Snowden  Eric Emerson Schmidt  Nation State Actor  Mary Ann Davidson  Julian Paul Assange
We have been warned ...
We have been warned ...

We buy all the tools...
We have been warned ...

We buy all the tools...

We've got the intel...
We have been warned...

We buy all the tools...

We’ve got the intel...

We fight the good fight!
We Protect Our Perimeter
The Nation State Actors are Coming!

Holy Firewall, Blogger-Man!
I. War will be more common in periods when *conquest is easy, or is believed easy*, than in other periods.

II. States that have, or believe they have, *large* offensive opportunities or *defensive vulnerabilities* will initiate and fight more wars than other states.

III. 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.
Feeling Vulnerable?
Feeling Vulnerable?

Security by 默默无闻
Feeling Vulnerable?

- What infrastructure is considered military?
  - Who paid for ARPANET?
- Is utility infrastructure always civil? Why?
- What is "relevant to national security"?
- Is the concept of CI flawed?
  - Which system is worthless?
Is this Cyber-War?

- Agreed Procedure for the Opening of Hostilities according to the Hague Convention (III) of 1907
  - Additional UN Security Council voting for UN members
- Jus in bello: Geneva Conventions now apply
  - Right of self-defense can be invoked
  - NATO Art. 5, mutual defense clause, option for members
- Computer based sabotage (e.g. Stuxnet) is argued to constitute “use of force” in the Tallinn Manual
  - Aggressor state(s) in violation of principles listed in Article 2 (1), (3) and (4) of the UN Charter
- Espionage is not proscribed internationally
  - Practice of secretly gathering information about a foreign government, a competing industry or individual

Feeling Vulnerable?

- What infrastructure is considered military?
  - Who paid for ARPANET?
- Is utility infrastructure always civil? Why?
- What is "relevant to national security"?
- Is the concept of CI flawed?
  - Which system is worthless?

Critical Infrastructure
Advanced = it worked
Persistent = repeatedly
Threat = you don't know why

Side note: Either China has the coolest Metasploit UI known to man, or these soldiers are, in fact, playing a game.
“Code of Conduct” proposed to UN 2011-09-12, 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”

"Superior firepower is an invaluable tool when entering negotiations."
General George S. Patton
Holy Arms Race, Vladimir!

APT? It's called ABT!
Автомат Калашникова

Ботнет
They have cyber-weapons!
They have cyber-weapons!

Let's control those!
Let's control those!

They have cyber-weapons!

Bugs are US Military!

Filed by Rear Admiral Grace Murray Hopper, US Navy
Surveillance is Security, Privacy needs it!

They have cyber-weapons!

Let's control those!

Bugs are US Military!

Surveillance is Security, Privacy needs it!

Filed by Rear Admiral Grace Murray Hopper, US Navy
Cat 4:

"Intrusion software": "Software" specially designed or modified to avoid detection by "monitoring tools", or to defeat "protective countermeasures", of a computer or network-capable device, and performing any of the following:

a) The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or

b) The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.
Cat 4:
"Intrusion software": "Software" specially designed or modified to avoid detection by "monitoring tools", or to defeat "protective countermeasures", of a computer or network-capable device, and performing any of the following:

a) The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or

b) The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.
5. A. 1. j.

IP network communications surveillance systems or equipment, and specially designed components therefor, having all of the following:

1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone):
   a) Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1));
   b) Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and
   c) Indexing of extracted data; and

2. Being specially designed to carry out all of the following:
   a) Execution of searches on the basis of 'hard selectors'; and
   b) Mapping of the relational network of an individual or of a group of people.

Note 5.A.1.j. does not apply to systems or equipment, specially designed for any of the following:
   a. Marketing purpose;
   b. Network Quality of Service (QoS); or
   c. Quality of Experience (QoE).
Surveillance Makes Vulnerable

Mount Watch More

Surveillance Makes Vulnerable
The Law Demands...
The Law Demands...

... There Shall be LI
The Law Demands...

- MPLS, PBR and SLB break
- LI-only ACLs: IDS off
- SSO unsupported
- Hard limits on bandwidth, sessions and VoIP calls
- Just another IP stack in the path
  - "Fragmentation" translates to "LangSec||GTFO"

And It Shall Be VRF
And IPv5 Shall Be Called Laser

The Law Demands...

- MPLS, PBR and SLB break
- LI-only ACLs: IDS off
- SSO unsupported
- Hard limits on bandwidth, sessions and VoIP calls
- Just another IP stack in the path
  - "Fragmentation" translates to "LangSec||GTFO"

... There Shall be LI

And It Shall Be VRF
Punting Takes Time
Punting Takes Time

Everywhere
No matter how big you are
Eventually, it's lethal
No matter how big you are
Punting Takes Time
Everywhere
What About Security Research?
Holy Spitefulness, Clippy!

Well Done, Retired Expert!
- **Bug**, in software, is an error, flaw, mistake, failure, or fault in a computer program or system producing an incorrect result, or causes unintended behavior.
- **Vulnerability**, in computer security, is a weakness allowing 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 a predictable way.
Bug, in software, is an error, flaw, mistake, failure, or fault in a computer program or system producing an incorrect result, or causes unintended behavior.

Vulnerability, in computer security, is a weakness allowing 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 a predictable way.
Bug, in software, is an error, flaw, mistake, failure, or fault in a computer program or system producing an incorrect result, or causes unintended behavior.

Vulnerability, in computer security, is a weakness allowing 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 a predictable way.

Definitions Matter!

It saves so much money!
- **Bug**, in software, is an error, flaw, mistake, failure, or fault in a computer program or system producing an incorrect result, or causes unintended behavior.
- **Vulnerability**, in computer security, is a weakness allowing 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 a predictable way.

**Definitions Matter!**

- **Bug**, in software, is an error, flaw, mistake, failure, or fault in a computer program or system producing an incorrect result, or causes unintended behavior.
- **Vulnerability**, in computer security, is a weakness allowing 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 a predictable way.

**Full Disclosure**

- Full Disclosure was invented to force software vendors into fixing vulnerabilities
  - ISO/IEC 30111 and 29147
- Many of the tools we have come to depend on are themselves dependent on a working full disclosure culture
  - Vulnerability scanners, penetration testing frameworks, IDS, IPS, threat intelligence services
- Second- and higher order dependencies
  - Testing, certification, regulatory requirements, ...

**The Cost it Saves!**

**How Convenient!**
Once Exploits Were Outlawed
Only Outlaws Had Exploits

Total Numbers

CORE Exploits Remote

Fraction of CVEs

CORE Exploits Remote

CORE Exploits Client

CORE Exploits Client
1. Players are asked to collect Bomb and Shrapnel splinters to save these causing damage to the Mowing Machines.

2. In Competitions, during gunfire or while bombs are falling, players may take cover without penalty for ceasing play.

3. The positions of known delayed action bombs are marked by red flags at a reasonably, but not guaranteed, safe distance there from.

4. Shrapnel and/or bomb splinters on the Fairways, or in Bunkers within a club's length of a ball, may be moved without penalty, and no penalty shall be incurred if a ball is thereby caused to more accidentally.

5. A ball moved by enemy action may be replaced, or if lost or destroyed, a ball may be dropped not nearer the hole without penalty.

6. A ball lying in a crater may be lifted and dropped not nearer the hole, preserving the line to the hole, without penalty.

7. A player whose stroke is affected by the simultaneous explosion of a bomb may play another ball from the same place. Penalty one stroke.

Holy WWII, CISO!

Shall We Just Deal With It?
Holy Riddle, Horn or Whistle?

On Blowing Things
Whistle-blowing (legal definition): "The disclosure by a person, usually an employee in a government agency or private enterprise, to the public or to those in authority, of mismanagement, corruption, illegality, or some other wrongdoing."

Recent "calls to action" use the term to mean disclosure on grounds of idealistic reasoning

- Belief models are fragile, easy to influence by third parties
- If law is not the differentiator between whistle-blowing and betrayal, what is?
  - What good is law for, if it's not defining border-lines?

What alternatives are proposed to the model of "humans trusting humans"?
What To Believe?
One blog always posts lies, the other always the truth. Both blogs give you directions: One will lead you to fulfillment, glory and fame – the other to an airport... You may post a single question at one of the blogs. Which question do you post?

What To Believe?

The Internet Lies
One blog always posts lies, the other always the truth. Both blogs give you directions: One will lead you to fulfillment, glory and fame – the other to an airport...
You may post a single question at one of the blogs. Which question do you post?

Prisoners' Dilemma's optimal strategy is to always defect
  But isn't it the wrong model?
  Life tends to be repetitive
Robert Axelrod experimentally determined the conditions for successful Iterated Prisoners' Dilemma strategies as being: Nice, Retaliatory, Forgiving, Non-Envious
One blog always posts lies, the other always the truth. Both blogs give you directions: One will lead you to fulfillment, glory and fame – the other to an airport...

You may post a single question at one of the blogs. Which question do you post?

- Honey trap; great option. Very successful.
- Blog writing: Has worked on a number of different Ops. [...]
- Discredit a company [organization, individual]
  - Leak confidential information to others or the press via blogs [or Twitter, mailing list, etc.]
  - Post negative information on appropriate forums
- Get another country to believe a 'secret'
  - Provide 'secret' information through an online agent
- Infiltration work
  - Acquire credibility with online groups

Source: JTRIG presentation allegedly leaked by Edward Snowden
Global Peace Index 2011

States of peace:
- Very high
- High
- Medium
- Low
- Very low
- Not included

Source: Economist Intelligence Unit.

Holy World Map, Sherlock!

Methods, Motives, and Identities
Sharing A Point?
Jul 2013: "Now increasingly we see that it's happening **domestically** and to do that they, the NSA specifically, targets the communications of everyone."

"But I sitting at my desk certainly had the **authorities** to wiretap anyone [...] even the President if I had a personal e-mail."
Jul 2013: "Now increasingly we see that it's happening **domestically** and to do that they, the NSA specifically, targets the communications of everyone."

"But I sitting at my desk certainly had the **authorities** to wiretap anyone [...] even the President if I had a personal e-mail."

"For fiscal 2013 [...] product revenue in the APJC segment increased by 3%. [...] offset by product revenue declines of 5% in China and 7% in Japan, reflecting certain challenges that we faced in these countries during portions of fiscal 2013, most notably in the fourth quarter of fiscal 2013."

Cisco Filing Nov. 2013
"For fiscal 2013 [...] product revenue in the APJC segment increased by 3%. [...] offset by product revenue declines of 5% in China and 7% in Japan, reflecting certain challenges that we faced in these countries during portions of fiscal 2013, most notably in the fourth quarter of fiscal 2013."

Jul 2013: "Now increasingly we see that it's happening **domestically** and to do that they, the NSA specifically, targets the communications of everyone." "But I sitting at my desk certainly had the **authorities** to wiretap anyone [...] even the President if I had a personal e-mail."

---

1. **People's Republic of China**
   - Prestige, intel, trolling, all without any diplomatic fallout
   - New perception of "Western Products" pushes CN brands
   - Anything questionable ever discovered in Chinese products from now on can be blamed on the US/NSA

2. **Russian Intelligence Services**
   - Служба специальной связи и информации, Спецсвязь России (Spetssviaz, aka FSO)
   - Служба внешней разведки Российской Федерации (СВР)

3. **The chosen few with access to the documents or person**
   - Plus their selected friends and new friends, respectively

4. **Anyone capable of accessing mounted TrueCrypt volumes or getting passwords of journalist laptops in hotels**

---

Cisco Filing Nov. 2013
Surveillance Jeopardy

- 100: Staff at this global observer needs no authorization for data access, since abuse never occurs.
- 200: This entity legally monitors every communication accessible, worldwide.
- 300: Internationally funded by the people, this organization doesn't pay any notable taxes.
- 400: An OP that social engineered code into ~66% of the top 10k websites, augmenting 37 signals from the source with surveillance at destination.
- 500: A global superpower, famous for its mastery of economic moats, codenamed "free", which as defending it far upstream while enriching its own resources at the same time.
It looks like you're trying to search the Web.

Holy Page, Larry!

Global Commercial Surveillance
Once upon a time ...

... a search query would work the same
  ... for another person
  ... on another computer
  ... on another day
... a "sort by relevance" feature tried
  sorting by relevance for the user
... blind people loved the Internet
Once upon a time ...
... a search query would work the same
  ... for another person
  ... on another computer
  ... on another day
... a "sort by relevance" feature tried
  sorting by relevance for the user
... blind people loved the Internet
Once upon a time …

… a search query would work the same
  … for another person
  … on another computer
  … on another day

… a "sort by relevance" feature tried
  sorting by relevance for the user

… blind people loved the Internet
Once upon a time ... 
... a search query would work the same
  ... for another person
  ... on another computer
  ... on another day
... a "sort by relevance" feature tried
  sorting by relevance for the user
... blind people loved the Internet

Remember Internet?

Remember Finding Stuff?

- E-commerce worked since 1979, on videotex
- In 1992, the U.S.G. allowed ARPANET to peer with commercial networks
  - 1993: Banners spotted on Web sites
  - 1994: SF-based AD-agency sells banner space
- But all the great businessman found only one thing they can reliably sell online
  YOU

Links to Actual Files?

Remember the War on Banners?
April 29, 2014 (WLS) -- The ABC7 I-Team is learning more about the "heartbleed virus" and how you can be a victim without even knowing it.

The popular software used to protect your personal information has been compromised, but that threat is confusing some people.

This not something you should blow off.

Technology experts say that the "Heartbleed Virus" is widespread and hit 66 percent of all websites over the past two years.

So the I-Team wanted to know what people are doing to stop the bleeding.

Heartbleed. The term comes from the communication between two so-called "hearts" on a server which verify your security as you shop, check e-mails and bank statements. There is now a backdoor break-in between those hearts, and it's bleeding.
The more idiots babble, the more you should trust your nerds.

Paraphrasing Jean-Paul Sartre
What do you mean $2.053 \times 10^9$ p.a. prove Alan wrong?

Holy Halting Problem, Peter Norton!
The Industry Got Your Back
The Industry Got Your Back

Just Believe!
The Industry Got Your Back

Just Believe!

A Business of Trust
Heartbleed? Sorry! That's Open Source.

The Industry Got Your Back

Just Believe!

A Business of Trust

Heartbleed? Sorry! That's Open Source.
I'm not upset that you lied to me.

I'm upset that, from now on, I can't believe you.

Friedrich Wilhelm Nietzsche
Holy Kernel Code, Vendor-Man!

You absolutely had to monitor over 500 protocols at Line Speed?
<table>
<thead>
<tr>
<th>unique</th>
<th>military grade</th>
<th>invisible</th>
<th>cyber</th>
<th>Snowden</th>
</tr>
</thead>
<tbody>
<tr>
<td>undetected</td>
<td>zero day</td>
<td>SCADA</td>
<td>APT</td>
<td>detection</td>
</tr>
<tr>
<td>preventing all</td>
<td>safely</td>
<td>BINGO</td>
<td>automatic</td>
<td>before</td>
</tr>
<tr>
<td>adaptive</td>
<td>malware</td>
<td>encryption</td>
<td>line speed</td>
<td>next</td>
</tr>
<tr>
<td>sandbox</td>
<td>unbreakable</td>
<td>impossible to compromise</td>
<td>proactive</td>
<td>certified</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>honeypot</td>
</tr>
</tbody>
</table>
Holy Software Quality, Vendor-Man!

You are making it worse!
The "Finding Yourself in a Hole" Manual
Chapter 1: STOP DIGGING
Regulation is Easy - And #FAILs

```
OB
tain "cyber security trends and implications" FROM regulator AS report
FOR EACH sector IN report:
    FOR EACH consumer_trend IN sector:
        SET vendor.fail TO unknown
        FOR EACH vendor MARKETING FOR consumer_trend:
            FOR EACH product MARKETED BY vendor:
                IF NOT product.isReported THEN
                    SET vendor.illegal TO true
                END IF
                CALL BSI.LocalAgencyEquivalent WITH product RETURNING verdict
                IF verdict < acceptable_threshold THEN
                    SET vendor.fail TO true
                END IF // fail
            END FOR // product
        END FOR // vendor
    END FOR // consumer_trend
END FOR // sector
```
The Root Cause of It ALL
You Can't Do Anything

The Root Cause of It ALL
The Root Cause of It ALL

You Can't Do Anything

Oops

No Liability!
The Root Cause of It ALL

You Can't Do Anything

Oops

No Liability!

All You Have is Patches
How About Trying This New Method?

Don't Pile Stuff on Top of Broken Stuff
There is only one known Silver Bullet for Computer Security. It is sentient and suffers from consciousness.

People
Holy Hacker Hire, Mr. Government!

Investing in Real Security Solutions
<table>
<thead>
<tr>
<th>Fear Uncertainty &amp; Doubt</th>
<th>Business Due Diligence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Concern</strong></td>
<td><strong>Concern</strong></td>
</tr>
<tr>
<td>What happens if we</td>
<td>What happens if we</td>
</tr>
<tr>
<td>invest in developing</td>
<td>don't invest in</td>
</tr>
<tr>
<td>our people and then</td>
<td>developing our people</td>
</tr>
<tr>
<td>they leave us?</td>
<td>and they stay?</td>
</tr>
<tr>
<td><strong>Recommended action</strong></td>
<td><strong>Recommended action</strong></td>
</tr>
<tr>
<td>$60k/p.a. Product</td>
<td>$60k/p.a. Person</td>
</tr>
<tr>
<td>No liability &amp; fitness</td>
<td>Reasonable liability</td>
</tr>
<tr>
<td>Unknown gain</td>
<td>Measurable gain</td>
</tr>
<tr>
<td>Unknown risks</td>
<td>Known (to be annoying)</td>
</tr>
</tbody>
</table>

Are You Sure that Nobody Gets Fired for Just Buying a Box?
She's right.

Get Over It!
Welcome to Joint Forces Development!

Invite Her!
Holy Irony, a Yellow Box?

Or buy another product. That too will help. Someone.
Tools Require Skills
They Don't Replace Them
Whether we win is not what matters. The way we win is all that matters.

GAME OVER