Why I ❤ offensive work
Why I 🚫❤ offensive work

Confessions of a recovering Vuln-Dev

A personal (key)note

- 2018: After ~20 years of security: Decided to do a few years of … something else. Foolishly agreed to keynote OffensiveCon 2020 around May 2019.

- Very successful at not thinking about security since Jan 2019. What does one talk about when one has intentionally avoided the topic for 15+ months?

- Solution: Take all the rambling chats over drinks I’ve had in recent years and condense them into a talk.

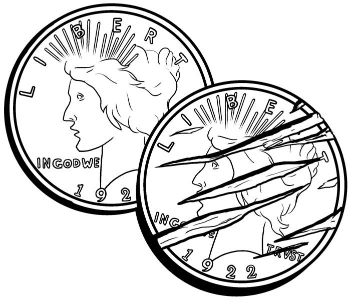
- I can’t have a drink with each of you individually to chat & bullshit, so this talk is the scalable version of “a random and rambling conversation over drinks”.

“A love / hate relationship with … everything”

- A person I worked with once asked:

“ Is it not very strenuous to have a love / hate relationship with …

… everything? “



DragoArt.com

- Security (both offensive and defensive) is a complex topic.

- This keynote: **A (very personal) recap of my complicated relationship with security**. I am sure almost everybody will find something to disagree with.

Why I ❤ offensive work

Reasons to ♥ offensive work

Technical reasons:

1. Full-stack CS, across abstraction layers
2. Creativity
3. Scientific frontiers
4. Practical real-world effects

Economic reasons:

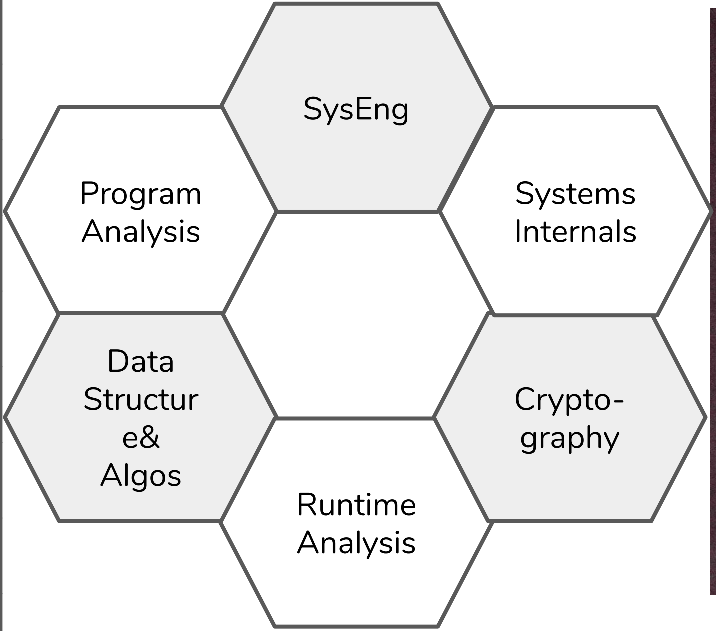
5. Incentive alignment
6. Mission-critical for customers
7. Not the customers money

Emotional reasons:

8. The “high” after success
9. Close to real-world magic
10. Interesting people

Technical ❤ 1: Full stack CS

- Interaction Software → World
- Higher Level Logic
- Software implementation
- Libraries
- Runtimes
- Operating System
- Firmware
- Hardware Spec
- Hardware Implementation



SysEng

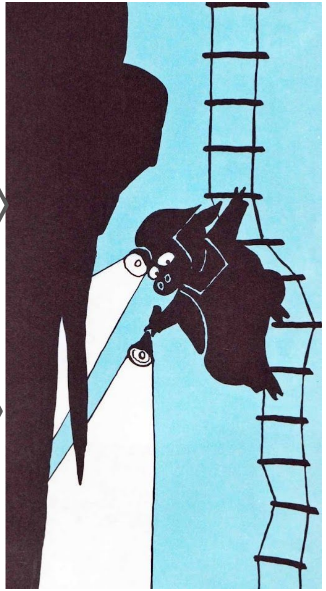
Program Analysis

Systems Internals

Data Structur e& Algos

Crypto- graphy

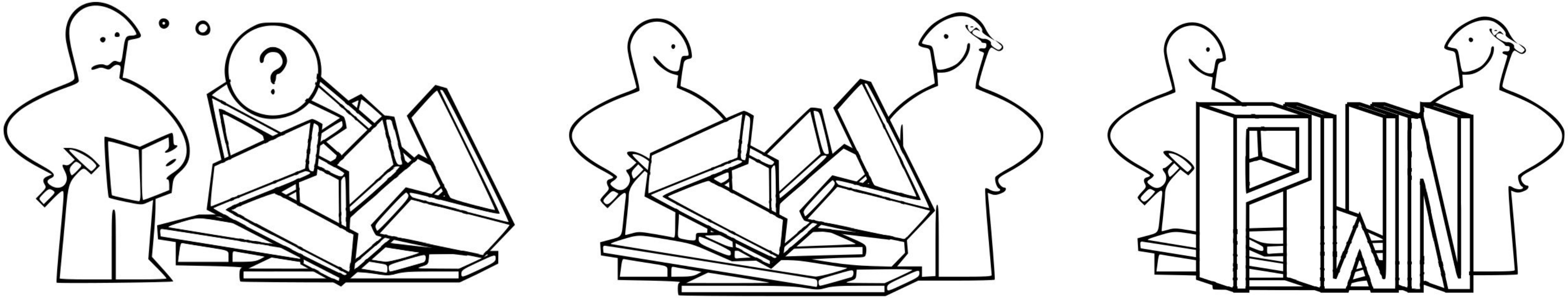
Runtime Analysis



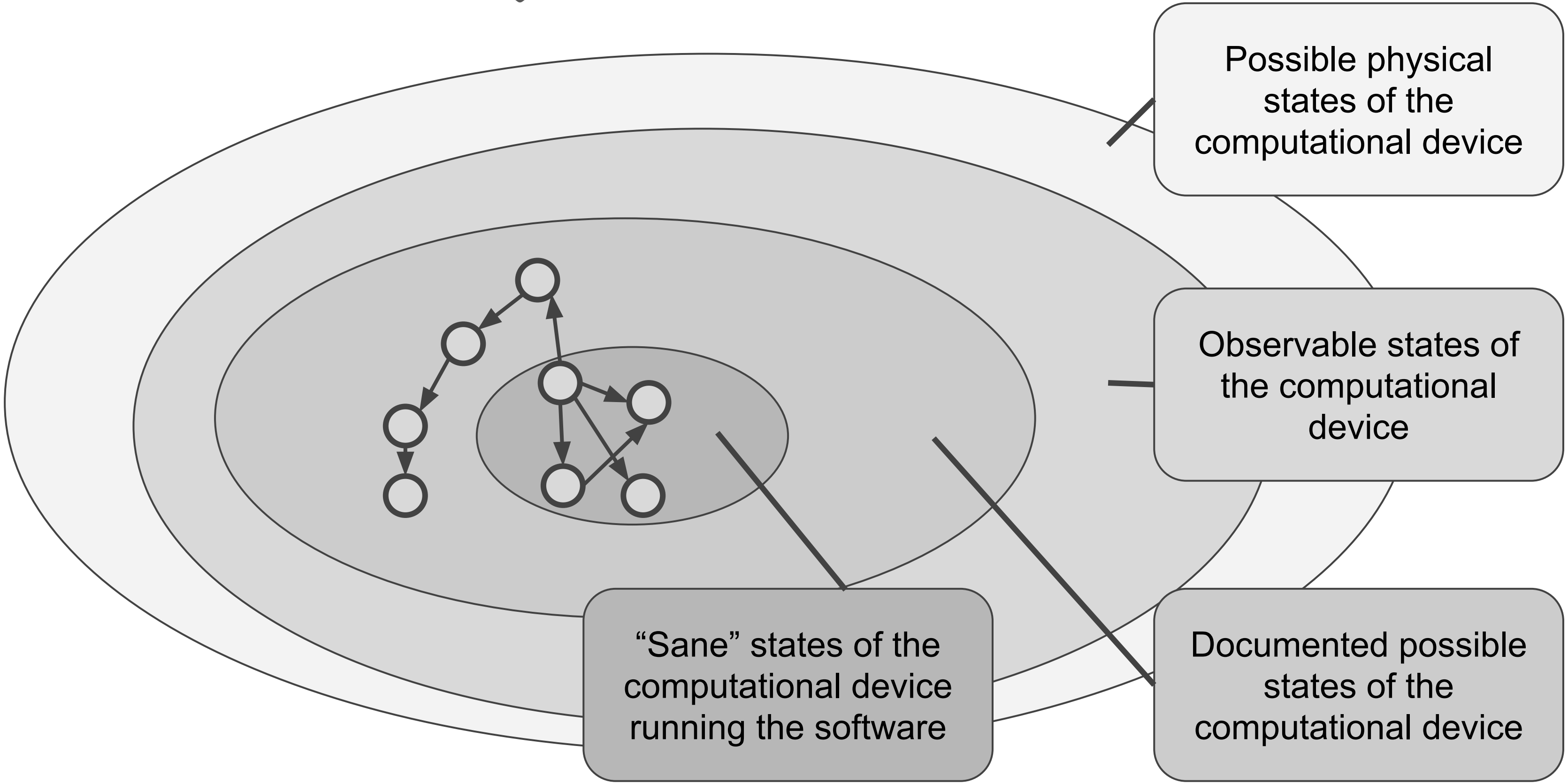
Spelunking in code caves & ruins

Technical ❤ 2: Creativity

- Analogy: Writing an exploit is like getting a random assortment of IKEA parts…
- … with the task of building a useful, sturdy, and comfortable chair out of it.



Technical ❤ 3: Scientific frontiers



Possible physical states of the computational device

Observable states of the computational device

Documented possible states of the computational device

“Sane” states of the computational device running the software

Technical ❤ 4: Practical effects

- Work on offensive technology is not theoretical.
- Contrary to work in (public) Cryptography, you can actually see the results: A root shell speaks to me differently than lowering the complexity of an attack from 2^128 to 2^110.
- Deeply satisfying to see the technology work.
- **Offensive tools are an outlier in the security (product) industry: They reliably do what they advertise they do.**

Economic ❤ 5: Incentive alignment

- Offensive work has near-perfect incentive alignment:
  - Success is 100% objectively measurable and discrete. It works or it does not work.
  - Technical excellence generates the income, and is directly measurable.
  - **This is exceedingly rare in most fields!**

- The opponent (vendors) **does not care (much) about fighting you**. They do care about wide adoption. If you have a bug in their software, your incentives are partially aligned.

- **“All offensive problems are technical problems.”** - so if your passion is solving technical problems, offensive work is a great playground.

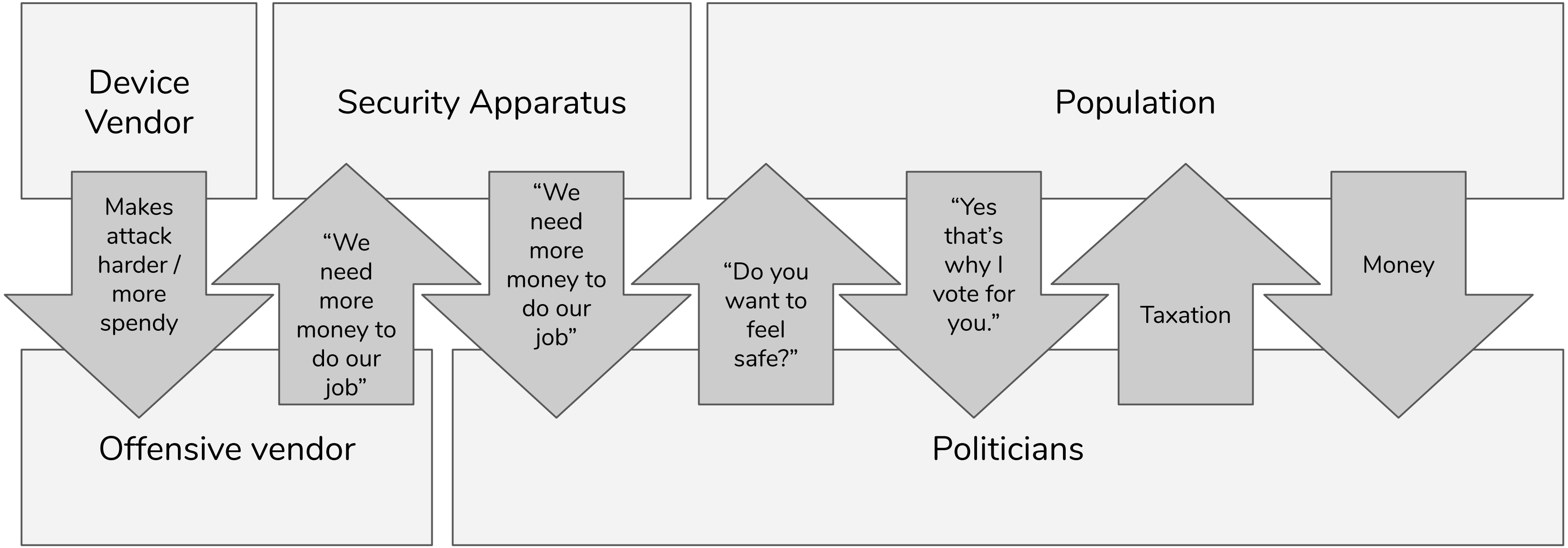
Economic ❤ 6: Mission-critical for customers

- The most important jobs, and the best products, are those that are mission-critical for customers. If your product is necessary for your customer to do their job, it's a good product.

- **Most security products are nice-to-have. The business can continue without them.** This is why defensive security is sales-driven, and this is why we have RSA as a conference.

- **Offensive security is mission-critical for customers**, which greatly reduces the need to explain to the customer why they want to buy it.

Economic ♥ 7: Not the customers money



Device Vendor

Security Apparatus

Population

Makes attack harder / more spendy

“We need more money to do our job”

“We need more money to do our job”

“Do you want to feel safe?”

“Yes that’s why I vote for you.”

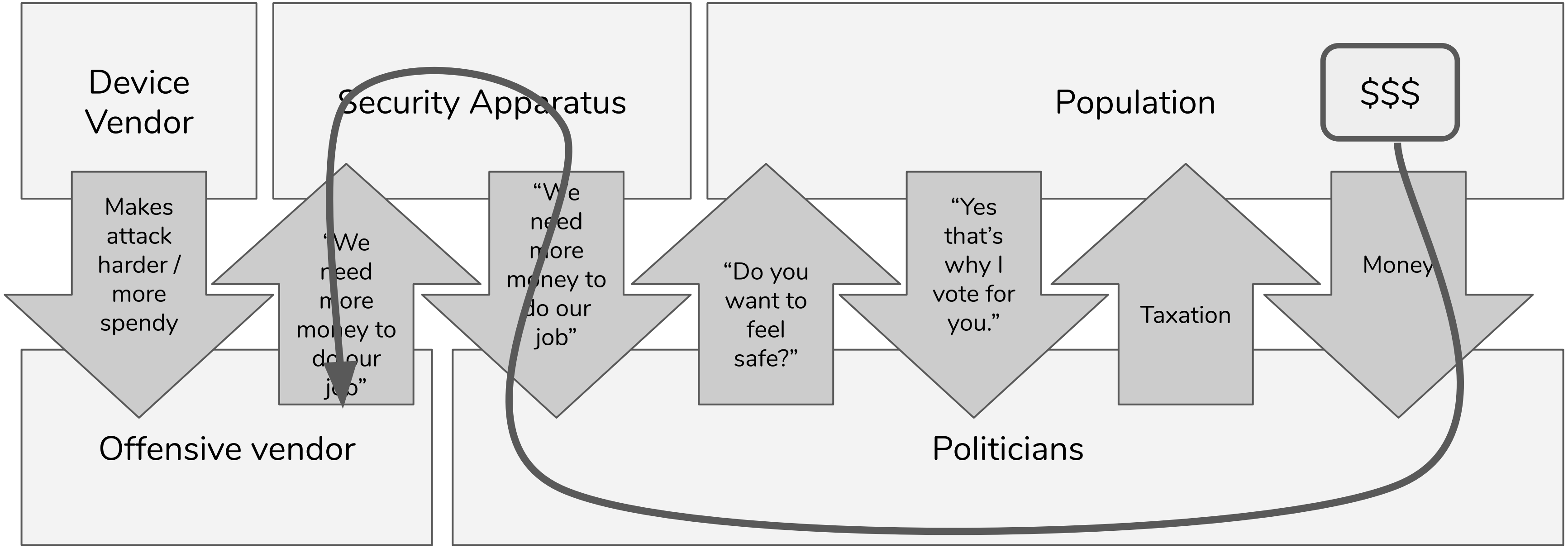
Taxation

Money

Offensive vendor

Politicians

Economic ❤ 7: Not the customers money


Device Vendor
Security Apparatus
Population
$$$
Makes attack harder / more spendy
"We need more money to do our job"
"We need more money to do our job"
"Do you want to feel safe?"
"Yes that's why I vote for you."
Taxation
Money
Offensive vendor
Politicians

The persons that provides the money is far removed from any idea of fair pricing, and has huge resources (all of the GDP). Improvements in vendor security can be transferred. Offense essentially becomes a tax.

Emotional ♥ 8: The high after success

- “The joy in mathematics is often the receding of the pain.”
- **Working on a difficult problem and finding a solution is inherently gratifying.**
- The discrete nature of offensive work means long periods of very little success, followed by a “jump” to “solution”.
- Very intense emotionally. Addictive even.

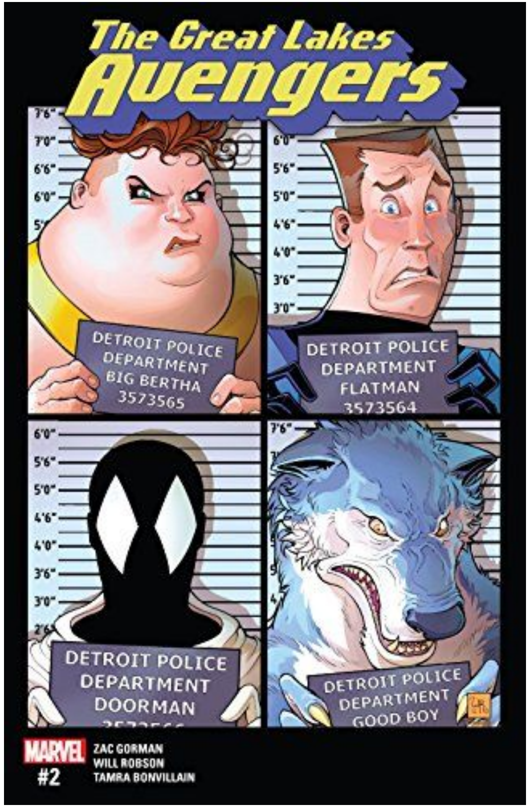
Emotional ❤ 9: Real-world magic

- Exploits are the closest thing to “magic spells” we experience in the real world: **Construct the right incantation, gain remote control over device.**

- Watching them work always feels like magic to me (even after interacting with them for 20+ years).

Emotional ❤ 10: The people

- Security used to be a backwater - and offensive security even more so.
- Most people one met were motivated by curiosity (or sense of duty) more than $.
- Extremely interesting community of misfits, often with very unique “mutant powers” and specialties.
- Lots of autodidacts with a passion for learning.


The Great Lakes Avengers
DETROIT POLICE DEPARTMENT BIG BERTHA 3573565
DETROIT POLICE DEPARTMENT FLATMAN 3573564
DETROIT POLICE DEPARTMENT DOORMAN
DETROIT POLICE DEPARTMENT GOOD BOY
MARVEL #2
ZAC GORMAN
WILL ROBSON
TAMRA BONVILLAIN

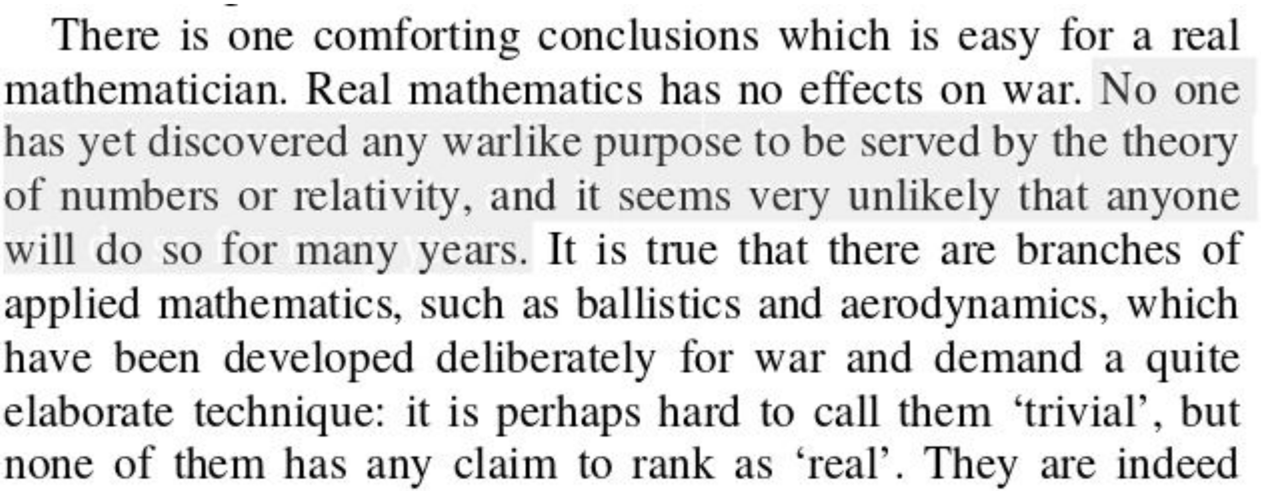
Detour 1: Science & Conflict

Can you do science without “helping” warfare?

Can you do science w/o helping warfare?

- I perceive myself as a scientist / engineer of sorts.
- Read Dürrenmatt's “The Physicists” and watched “Copenhagen” in my late teens (two plays that explore science, warfare, and their implications).
- Thought a lot about “making my living” essentially via military/intelligence budgets ca. 2000 onward.
- Often wondered: How can one prevent “one’s work falling into the wrong hands”? (Impressionable 14-year old me had listened too much Prodigy)

Example 1: Hardy’s “A Mathematician’s Apology”



There is one comforting conclusions which is easy for a real mathematician. Real mathematics has no effects on war. No one has yet discovered any warlike purpose to be served by the theory of numbers or relativity, and it seems very unlikely that anyone will do so for many years. It is true that there are branches of applied mathematics, such as ballistics and aerodynamics, which have been developed deliberately for war and demand a quite elaborate technique: it is perhaps hard to call them ‘trivial’, but none of them has any claim to rank as ‘real’. They are indeed

Published 1940

First nuclear bomb 1945

Clifford Cocks invented RSA-like crypto 1973

Example 2: Social Anthropology

- I dated a Social Anthropologist in the early 2000s
- She made fun of the fact that both Mathematics and CS were thoroughly militarized disciplines.
- 2007: Secretary of Defense Gates starts "Human Terrain System"
- DoD uses Anthropologists etc. to improve warfare capabilities in Iraq

Claim: You can’t control the use of knowledge

- The choice is not between “peaceful” and “warlike” science. For most of science, the only choice is “relevant” and “irrelevant”.

- Only way to make sure your scientific output will not be used by the military for war: Make sure it **irrelevant**, or **wrong**, or better: **Both**.

- Almost anything that will give one side an advantage will eventually be used in warfare.

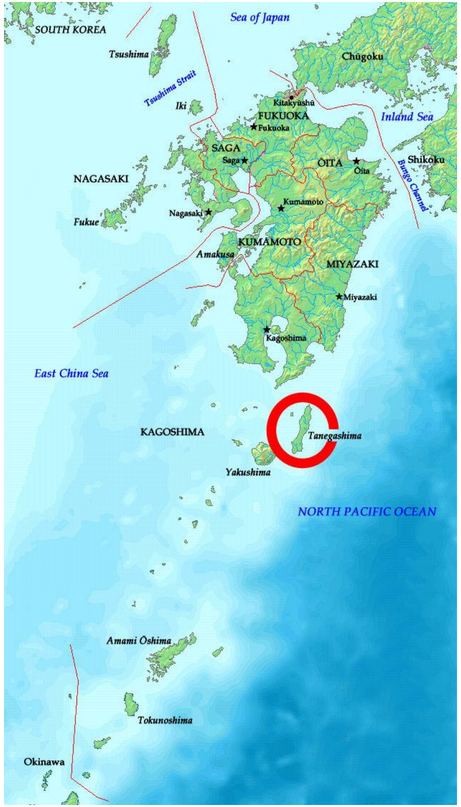
- Nonetheless: **The individual still has the responsibility to judge what they are working on.** This is often not easy.

Detour 2: Science & Conflict

Is it immoral to improve weaponry?

Are better weapons bad?

- People are inclined to believe that better weapons are (morally) bad.
- I visited Japan in early 2016 - both Hiroshima and Tanegashima.
- I will not talk about Hiroshima. Visit it if you can; particularly if you think you work in “Cyberwar”.
- Tanegashima is an island in the south of Japan

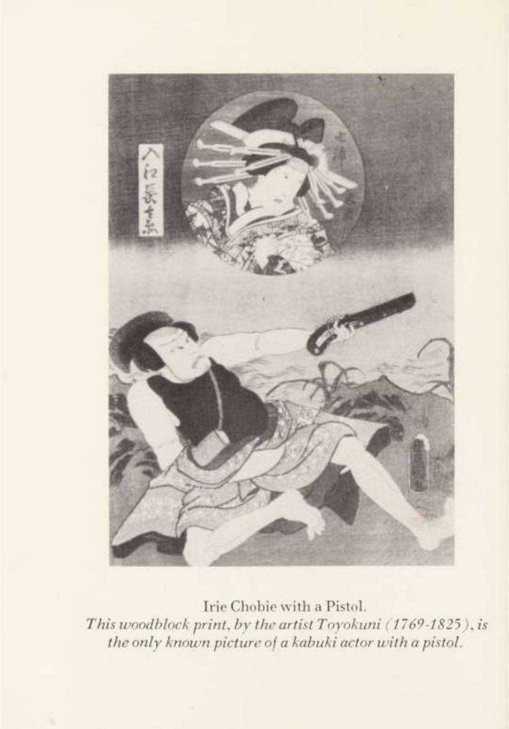


Are better weapons bad?

- 1467: Japan’s Feudal system collapses. Sengoku period starts, permanent internal warfare. No side could get an upper hand.

- 76 years later, the first Musket arrives in Japan (1543). Full adoption into the battle around 1570s; decisive in battle from 1575.

- From 1615 onward: Japan unified, century of peace. **108 years of war, ended in 40 years**.



Irie Chobie with a Pistol.
This woodblock print, by the artist Toyokuni (1769-1825), is the only known picture of a kabuki actor with a pistol.

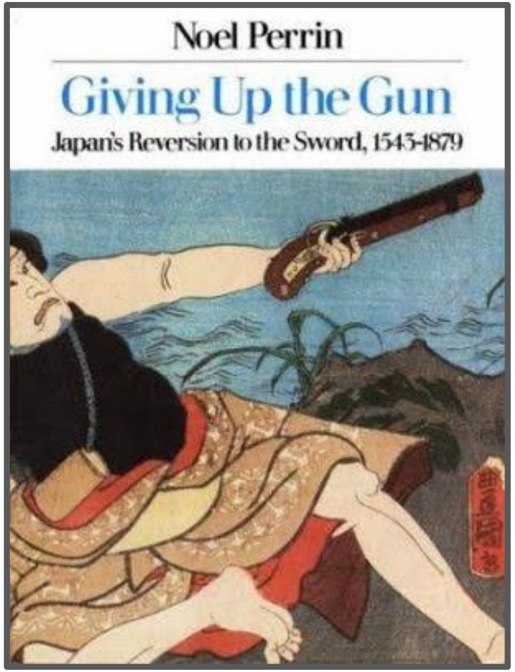
Are better weapons bad?

- Prolonged warfare is terrible.
- **Superior weaponry does not always mean more civilian casualties.**
- Some people argue that the terrible power of nuclear weapons are what enabled the last 75 years without World Wars.

I do not have an answer.
I think about the history of Tanegashima, with little result.

Are better weapons bad?

- Counterexample: In New Zealand, the arrival of guns led to significantly deadlier warfare.
- Interestingly, Japan also de-armed itself afterward.
- Gradual rejection, even “forgetting” about how to manufacture guns.
- Unsure what the lesson is, except “weapons are always net bad” is too simplistic.



Detour 3: Fragile Democracies

100 years without death squads?

My sabbatical experience (2015-2016)

- Almost every place I visited had **living memory** of death squads:
  - **France** (Algerian independence war - OAS, Death flights, etc.)
  - **Morocco** (742+ “disappearances” under King Hassan II)
  - **Uruguay** (20% of population arrested at one point under dictatorship, 180+ killed)
  - **Argentina** (between 9k and 30k people “disappeared”)
  - **South Africa** (Vlakplaas death squads)
  - **Portugal** (PIDE murders under Salazar)
  - **Spain** (100k-200k dead in the White Terror under Franco, 100k “disappeared”, GAL)
  - **Taiwan** (“Iron Blood Patriots”, Martial Law, Kaohsiung Incident)

My sabbatical experience (2015-2016)

- Takeaway: Democracy and basic rights are **fragile**, and **not the norm**.

My sabbatical experience (2015-2016)

- Takeaway: Democracy and basic rights are **fragile**, and **not the norm**.
- **Every democracy is ~2 terror strikes and 1 opportunist away from dictatorship.**

My sabbatical experience (2015-2016)

- Takeaway: Democracy and basic rights are **fragile**, and **not the norm**.
- **Every democracy is ~2 terror strikes and 1 opportunist away from dictatorship.**
- Empirically, state-sponsored death squads happen with regularity.

My sabbatical experience (2015-2016)

- Takeaway: Democracy and basic rights are **fragile**, and **not the norm**.
- **Every democracy is ~2 terror strikes and 1 opportunist away from dictatorship.**
- Empirically, state-sponsored death squads happen with regularity.

Most of us have grown up in an unusually peaceful time in an unusually peaceful part of the world. Being conscious of that is important. It certainly biases decision-making.

Why I 🚫❤ offensive work

Reasons to 🚫♥ offensive work

Societal reasons:

1. “For whom” - you always pick a side
2. Non-optimal choices for employers
3. Limited societal value-add

Emotional reasons:

4. Every. Single. Moral. Question. Is. Complicated.
5. Economic incentives cloud judgement of one’s actions.
6. Non-accumulative.

Technical reasons:

7. Repetitive when maximizing profit
8. Become the world’s leading expert on obsolete technologies
9. Missing a huge technical transformation
10. The obituary test

Societal 💔 1: “For whom?” - you pick a side

- Bob Morris Sr. asked me when I met what I do. “I study math.” - “For whom?”

- All of security is fundamentally about **human power & conflict**. You always pick a side.

- Interestingly, both **defensive and offensive security tends to be on the side of the already-powerful.** I am running out of sides I like to pick.

Societal 2: Career paths with downsides

Three possible employers for offensive work with different pro's and con's.

Government agency	Offensive vendor	Defensive vendor

Societal 2: Career paths with downsides

Three possible employers for offensive work with different pro's and con's.

Government agency:

PRO: Impactful, direct insight in use of your work.

CON: Comparatively low pay.

CON: Onerous travel restrictions. No work from home.

CON: Career advancement often means less tech work.

CON: May end up managing contractors.

Societal 2: Career paths with downsides

Three possible employers for offensive work with different pro's and con's.

Offensive vendor:

PRO: Better salaries.

CON: For many players, profit is maximized when restraint on sales is minimized (subject to other government threats). Selling to the scummiest maximizes profit.

CON: Insight into the use of your work is limited and often misleading (see HackingTeam)

CON: Legal protections unclear in the long run.

Societal 2: Career paths with downsides

Three possible employers for offensive work with different pro’s and con’s.

Defensive vendor:

PRO: Good salary (or less good salary but great flexibility in VRPs)

PRO: Fewer ethical mis-incentives.

CON: You are not business-critical.

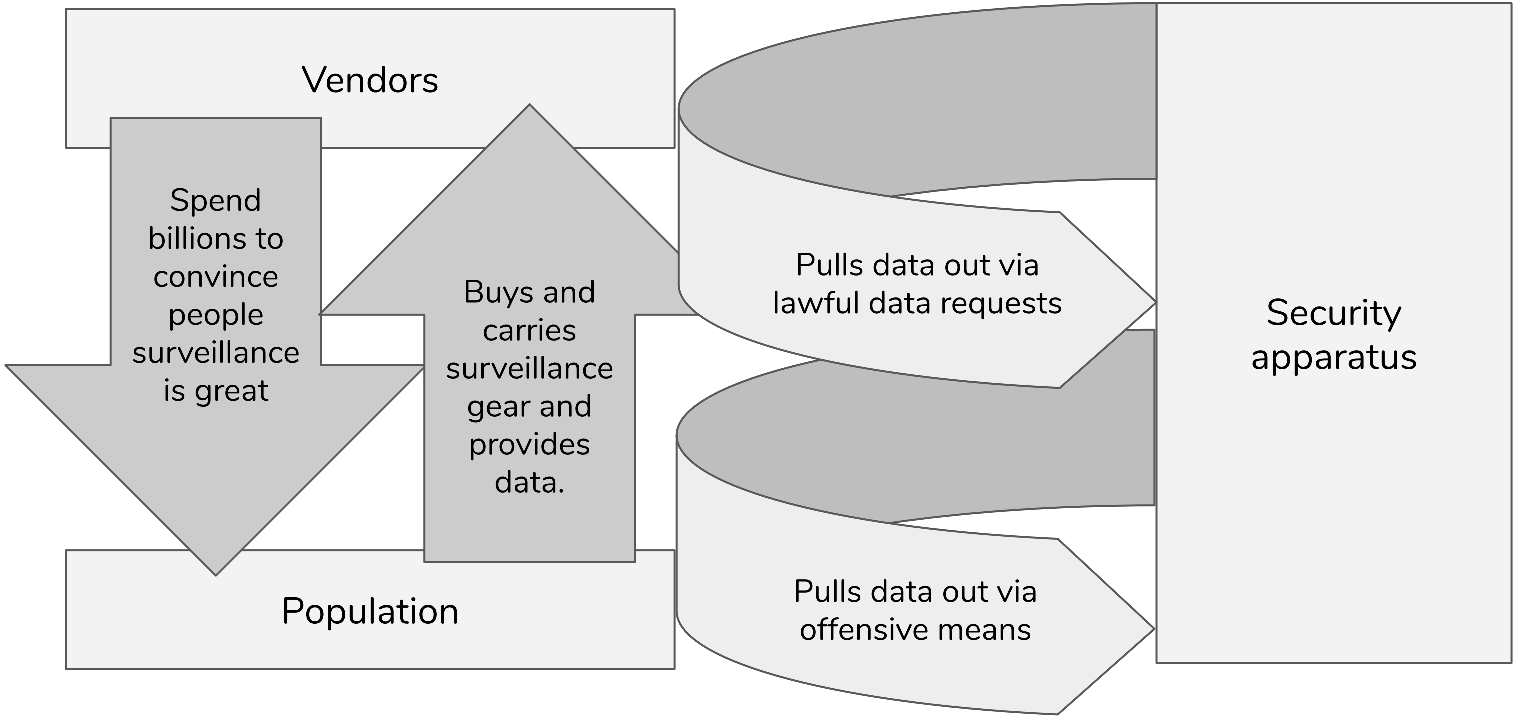
CON: You are always a cost-center.

CON: You get paid to “kill” your creations.

Societal 🚫❤ 3: Limited value-add

- Vendors have turned themselves into spy agencies (for ad-targeting etc.)
- Population pays for their own surveillance gear :-)
- Spy agencies want to have a piece of the pie.
- How does offensive work improve society or anyone’s life except mine?
- Potential for positive impact on millions of people: Often (not always) limited.

Societal 💔 3: Limited value-add


Vendors
Spend billions to convince people surveillance is great
Buys and carries surveillance gear and provides data.
Population
Pulls data out via lawful data requests
Pulls data out via offensive means
Security apparatus

optimyze

Emotional 💔 4: Everything is complicated

- The joy in bug discovery and exploitation is quite “pure”.
- Every decision thereafter can be turned into an entire bookshelf of moral philosophy PhD theses or gigabytes of Twitter nonsense.
- I do not enjoy those complications.

Emotional 5: Economics cloud judgement

- **“It is difficult to get a man to understand something when his salary depends upon his not understanding it.”**. People tend to pick their ideologies by function.

- By being economically dependent on offensive work, one impairs one’s judgement in thinking about it.

- I had the feeling that being “part of security” and making my living off of security was distorting my views, and curious about how my views would change without the distorting influence.

Emotional 6: Non-accumulative

- **Offensive security** is much less accumulative than many other parts of engineering.

- Working on tooling means 10 years down the line your tools are better.

- Looking back at a long offensive career is often: “I found this OpenSSH remote …. and it is gone. I found this RDP remote … and it is gone. I developed this technique for exploiting 2006 kxmalloc, and it was replaced.”

- Even by tech standards, offensive work is particularly ephemeral.

Technical 7: Repetitive at max profit

- **New targets have a significant ramp-up cost.** Finding and building your first Chrome remote is much more expensive than the next 10.

- Entire toolchains depend on “swappability” of parts.

- The learning effect on your 10th Chrome or Safari or iOS kernel bug is much less than on your first.

- You maximize profits when you also maximize boredom and stagnation.

Technical 8: Experts on obsolete tech

- **Obsolete technologies are where the bugs are.** There are more people that have deeply analyzed TrueType Font rendering virtual machines for vuln-dev than for typography.

- By definition, customers want to target “mass-market” tech. This is often much older than “emerging” tech.

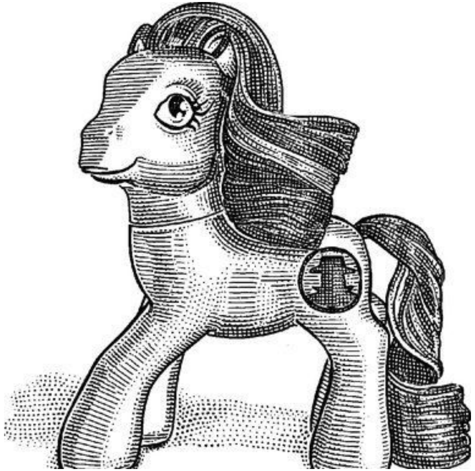
- Eventually, obsolete tech ceases to be useful even for offensive purposes. At this point, you are stuck with an encyclopedic knowledge of how TrueType font rendering bugs evolved from 1995 to now.

Technical 9: Missing a huge tech transform

- **Computing is changing** more rapidly right now than in recent decades.
- **Datacenter-sized computing** is emerging, with emergent proto-OS’s and nobody with any clue how to properly architect them. No full OS exists. No real debugging exists.
- **End-of-Moore** will reshape software deeply, and is already reshaping hardware deeply.
- **A lot of offensive work:** Another bug in Chrome plz kthxbai. Or perhaps “another Safari bug + iOS privesc plz kthxbai”. Feels unimportant / unexciting.

~~Technical~~ Emotional 10: The obituary test

- I believe in “reverse engineering your life from your obituary”.
- Imagine the obituary you would like to have - then live your life so you get it.
- When imagining my obituary, it felt like I should do something else for a while.
    - One of my idols, Gerardo Richarte, has a successful post-security career building imaging satellites.
    - Many other of my idols had multiple careers.
    - **Fear of being a one-trick Pwnie.**
    - (Can always return to security if all else fails)



Doing something else

- Decision on my side: Do something else for a while.

- Performance optimization has many of the technical upsides of offense:
  - Full stack computer science
  - Technical alignment of incentives:
    - Most interesting problems are technical
    - Good technical solutions translate to monetary savings easily
  - Extremely interesting problems
  - Lots of room for creative solutions

Doing something else

- Performance optimization has a few emotional advantages:
    - It is surprisingly liberating to not have ambiguous feelings about the implications of my work.
    - Not having to think about “for whom” is nice.
    - Success has a “positive externality” -- same GDP at less CO2.

- Not doing security has great advantages in Twitter debates
    - I can always accuse the other side of having an invalid opinion because their judgement is invariably clouded by their economic incentives.
    - On the other hand, my opinion is clearly truth, since I have no dog in the fight :-)

- Possibly economic disadvantages?
    - Unclear if it can be profitable - harder to “become a small tax on GDP”.

Summary

1. Offensive work is great.
2. Offensive work is terrible.

3. One should be mindful of the fragility of democracies and personal rights.
4. The ethical questions are real, and complicated, and have no easy answers.

5. Security is a tiny fragment of a much bigger real world.
6. Offensive work is just a tiny fragment of a much bigger computational world.

♥ **Vs** 🚫♥ **is a difficult balancing act. Enjoy the Con!**