It Wasn’t Supposed to Be Like This: Decelerate

1 November 2018

Jason Healey

InfoWarCon 2018

About Me

- Air Force
- Infowarcon
- Many suits
- Finance
- Government
- Policy
- Thinking and writing
  - Risk and conflict

What Many Thought

- Radically decentralize and disintermediate information and control
- Boost to economy, society, and humanity
- Preferentially boosts freedom and democracies
- Information wants to be free and routes around censorship
- Yes, there is a dark side, but they are fixable and we will fix them

> “Few if any contemporary computer security controls have prevented a [red team] from easily accessing any information sought.”
>
> Lt Col Roger Schell (USAF)

Roger Schell, “Computer Security: the Achilles’ heel of the electronic Air Force?” http://insct.syr.edu/wp-content/uploads/2015/05/Schell_Achilles_Heel.pdf

Biggest Losers

- Countless “wake up calls”
  - Cuckoo’s Egg, Morris Worm,
  - Eligible Receiver 97, Solar Sunrise, Moonlight Maze
  - Stuxnet, Buckshot Yankee, OPM
  - WannaCry, NotPetya…

Biggest Losers

- Countless "wake up calls"
  - Cuckoo's Egg, Morris Worm,
  - Eligible Receiver 97, Solar Sunrise, Moonlight Maze
  - Stuxnet, Buckshot Yankee, OPM
  - WannaCry, NotPetya…
- Plenty "enough is enough"
  - Cyber Sputnik moment
  - Cyber Manhattan Project
  - Cyber Moonshot
  - "Defensible Cyberspace"
  - SIPA-Atlantic Council: Cyber Recommendations Project

Important Defensive Innovations of the Past 50 Years

New York Cyber Task Force

SIPA

What kind of innovation is it?

Where is primary effect of the innovation?

		TECHNOLOGY		OPERATIONS		POLICY	
WITHIN ENTERPRISE Changes implemented by centrally managed IT team	PAST	**Computer and network passwords** (1960s-1980s) **Intrusion detection** (1990s) **Mass vulnerability scanning** (1990s) **Encrypted data & comms** (2000s) **Intrusion prevention** (2000s) **Hardware-based security** (e.g., TPM) (2000s) **Cloud-based architectures** (2010s) **Multifactor authentication** (2010s)	**Firewalls** (1980s) **Anti-virus/anti-malware** (1990s+) **Expedited deployment of patches** (1990s+) **Network segmentation** (2000s) **Malware sandboxing** (2000s) **Security analytics** (2000s) **User & entity behavioral analytics** (2000s) **DDoS protection** (2010s) **Tokenization** (2010s)	**User education and awareness** (1970s) **Creation of CERTs** (1980s) **Creation of ISACs** (1990s) **Training & certifications** (1990s) **Asset inventories** (2000s) **Top 20 controls** (2000s) **Board involvement, liability** (2010s) **Presumption of breach** (2010s) **NIST cyber framework** (2010s) **Intel-driven operations** (2010s)	**Creation of pentesting teams** (1970s) **Creation of CISO role** (1990s) **Capability Maturity Model** (1990s) **Response playbooks** (1990s) **Cyber exercises** (2000s) **Standard configurations** (2000s) **Cyber kill chain** (2010s) **Automated threat sharing** (2010s) **FBI sharing of IOCs** (2010s)	**Commission and task force reports** (e.g., Ware Report, PCCIP) (1970s+) **Cybersecurity laws** (e.g., CFAA) (1980s) **Single White House cyber official** (2000s) **State data breach laws** (2000s) **Recognition of cyber as operational/business risk** (2000s) **Board accountability including SEC guidance** (2010s) **USG disclosure to companies if they're breached** (2010s) **FTC enforcement actions** (2010s) **Enabling policies and laws** (e.g., Info. sharing, CISA, Exec. Orders) (1990s) **Leveraging existing regulations, as with finance sector** (FFIEC IT Handbooks, GLBA)	
	POTENTIAL FUTURE INNOVATIONS	Critical mass of cloud deployment Automated measurement of attack surface Computer-generated software diversity Widespread chip-and-pin deployment Scalable security automation	Autonomic and autonomous defenses Strong bio-authentication Alternate computing and security architectures (e.g., islets) Instrumenting data with sensors Analog controls	Security scorecards and ratings Active vendor management Insurance and other risk transfer Improved security metrics from cloud More holistic combination of risk, cybersecurity, physical security, business continuity, crisis management Software bill of materials		Safe harbor provisions for sharing National data breach notification law	
ACROSS CYBERSPACE AS A WHOLE 1. Change at end points that "floats all boats" 2. Change to "key terrain" like ISPs	PAST	**Automated updates** (1990s) **Built-in NAT firewalls** (1990s) **Adding security to s/w development lifecycle** (2000s) **Dev environment security** (2000s) **Security added to IETF standards process** (2000s) **OS hardening** (2010s) **Ubiquitous, transparent encryption** (2010s) **Cloud-based security at platform companies** (2010s) **Ubiquitous, secure protocols** (HTTPS, TLS/SSL) (2010s) **Automated testing** (2010s)		**Physical protection, personnel security and operational security** (1960s) **Creation of operators' groups** (e.g., NANOG, RIPE) (1990s) **Security certifications** (1990s) **Arresting malicious attackers** (1990s) **Volunteer groups for response** (e.g., Conficker, NSP-SEC) (2000s) **Volunteer groups for protection** (e.g., I Am the Cavalry) (2000s) **Rise of security industry and outsourced monitoring** (2000s) **Industry Associations** (e.g., ICASI, Cyber Threat Alliance, M3AAWG) (2000s) **Rise of DevOps** (2000s) **Institutionalized bug bounty programs** (2010s) **Attribution methodologies** (2010s) **Botnet Takedowns** (2010s)		**Education: Cybersecurity Core Curriculum, CAEs, NICE** (1990s+) **Budapest Convention** (2000s) **International capacity building** (2000s) **International coordination** (e.g., UN GGE, London and EWI processes) (2010s) **DMCA exemptions for security researchers** (2010s) **Law enforcement attachés** (2010s) **Vulnerabilities Equities Process** (2010s) **Indictments, sanctions** (2010s) **New USG orgs** (e.g., CS&C, NCSC, CTIIC) (2010s) **Scandinavian botnet policies and cleaning ecosystem** (2010s) **Australia ISP code of conduct** (2010s)	
	POTENTIAL FUTURE INNOVATIONS	Inexpensive formal methods, such as HACMS Formal methods applied to standards, like HTTPS Signed firmware Quantum encryption Blockchain		Cyber Independent Testing Labs and other quantification and rating systems Continuous disruption of adversary operations Independent attribution organization Crowdsourcing IOCs for early detection		Norms: rules of the road for cyber conflict "Naming and shaming," especially when norms are violated FCC action Regulatory emphasis on response, rather than protection	Global governance structure: G20+ICT20 Shifts in liability, especially for software and IoT Federal insurance backstop Improved security metrics to drive better policy WTO and trade restrictions

What reasons are there to think we can achieve any of this to stop our decades-long losing streak?

Even if we can, what else do we break?

Good Solutions Abound But…

- Most add significantly to complexity
- Most only deal narrowly with cyber
- Most make some *other* problem worse
  - – Platforms
  - – Liability
  - – Sovereign action

Good Solutions Abound But…

Complexity

- In a complex and interconnected system *you can never do just one thing*…
- Adding more complexity to cyber defenses likely only postpones a larger crash later

"… complexity hides interdependence(s), ergo complexity is the enemy of security"

Dan Geer

Dan Geer, Jr., A Rubicon, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1801, 5 February 2018, <https://www.hoover.org/sites/default/files/research/docs/geer_webreadypdfupdated2.pdf>.

“For fat-tailed variables, the mean is almost entirely determined by extremes. ‘If you are uncertain about the tails, then you are uncertain about the mean.’”

Dan Geer

Dan Geer, Jr., A Rubicon, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1801, 5 February 2018, <https://www.hoover.org/sites/default/files/research/docs/geer_webreadypdfupdated2.pdf>.
Pasquale Cirillo and Nassim Nicholas Taleb, “What are the Chances of a Third World War?” Real World Risk Institute Working Paper Series, accessed January 23, 2018, http://www.fooledbyrandomness.com /significance.pdf.

“The heavy tails that accompany complexity mean that while most days will be better and better, some days will be worse than ever before seen … complexity accumulates and unacknowledged correlated risks become embedded”

Dan Geer

Dan Geer, Jr., A Rubicon, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1801, 5 February 2018, <https://www.hoover.org/sites/default/files/research/docs/geer_webreadypdfupdated2.pdf>.

Good Solutions Abound But…

Cyber Only

- Even if we solve cybersecurity somehow…
- What about
  - Loss of privacy
  - Spread of false information
  - Balkanization
  - …

Spread of False Information

- Gresham’s Law
  - Bad money drives out good

Spread of False Information

- Gresham's Law
  - Bad money drives out good

Gresham's Law of Information:
Bad information drives out good.

Spread of False Information

- Gresham's Law
  - Bad money drives out good

Gresham's Law of Information:
Bad information drives out good.

Gresham's Law of the Internet: Bad information drives out good, fast and with malice, *you jerk*

Balkanization

- Not just traditional explanation of “splitting”
  - “Fifteen years after its first manifestation as a global, unifying network, it has entered its second phase: it appears to be balkanising, torn apart...”

https://www.economist.com/briefing/2010/09/02/a-virtual-counter-revolution

Balkanization

- Not just traditional explanation of "splitting"
  - "Fifteen years after its first manifestation as a global, unifying network, it has entered its second phase: it appears to be balkanising, torn apart..."
- But additionally:

Internet adversaries of all kinds are increasingly locked into the endless fighting in remembrance of ancient grievances

https://www.economist.com/briefing/2010/09/02/a-virtual-counter-revolution

Good Solutions Abound But…

Tradeoffs Make Other Problems Worse

- Free flow of information
- Too free a flow of information
- False information
- Trolling
- Privacy
- Free speech
- *Convenience*

- Computer and network security
- LE and national security
- Network neutrality
- Borders and sovereignty
- Inequality
- Innovation
- Investment

Solving for one induces predictable and unpredictable knock-on effects…

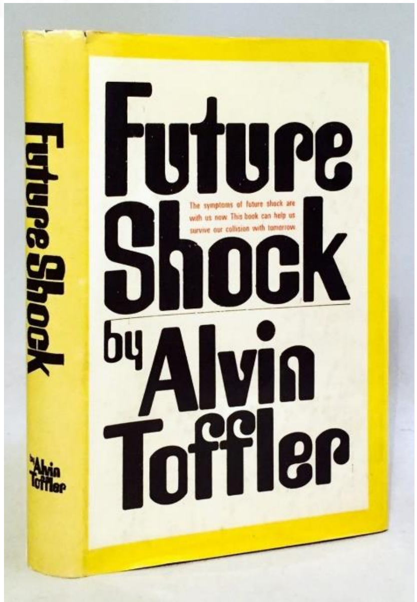
> “Whenever I run into a problem I can’t solve, I always make it bigger. I can never solve it by trying to make it smaller, but if I make it big enough I can begin to see the outlines of a solution.”
>
> Dwight D. Eisenhower

How to think about making the problem bigger?

Future Shock

“Future shock is the dizzying disorientation brought on by the premature arrival of the future.”

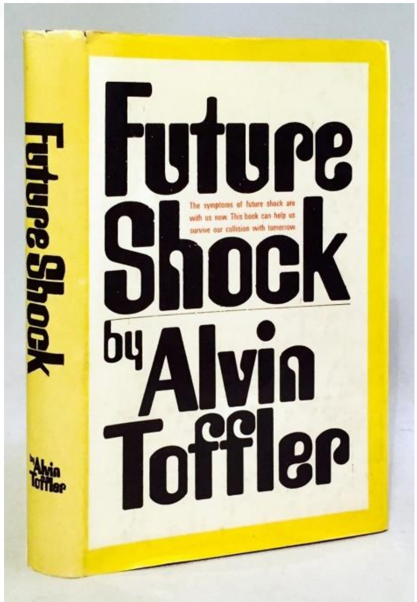
Alvin Toffler


Future Shock
The symptoms of future shock are with us now This book can help us survive our collision with tomorrow
Shock
by Alvin Toffler
Future Shock
by Alvin Toffler

1970

Future Shock

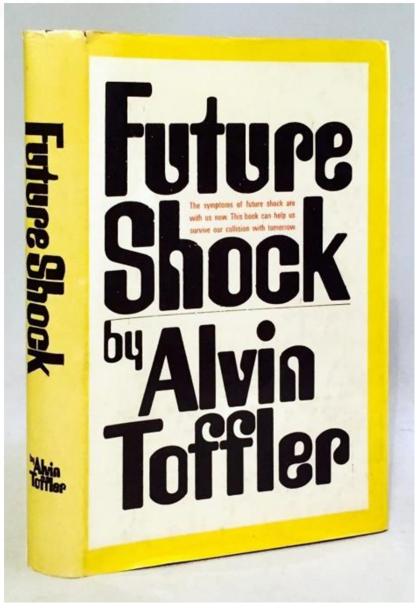
The 800th Lifetime…


Future Shock
The symptoms of future shock are with us now This book can help us survive our collision with tomorrow
Future Shock
by Alvin Toffler
Future Shock
by Alvin Toffler

Future Shock

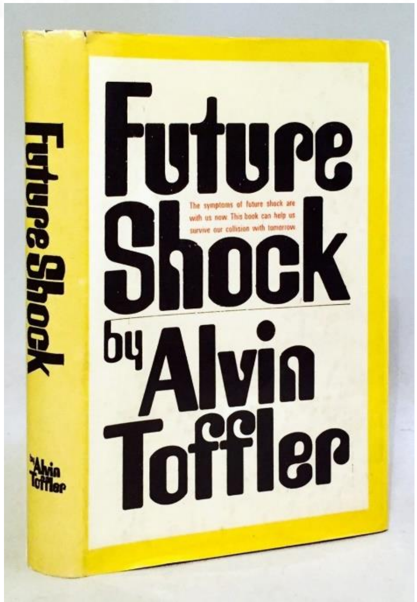
The 800th Lifetime…

- Out of caves 150 lives ago
- Only speak between generations 70 lives ago
- Only four to six with electric motors
- Most material goods only within last two or three


Future Shock
The symptoms of future shock are with us now. This book can help us survive our collision with tomorrow.
Future Shock
by Alvin Toffler
Alvin Toffler

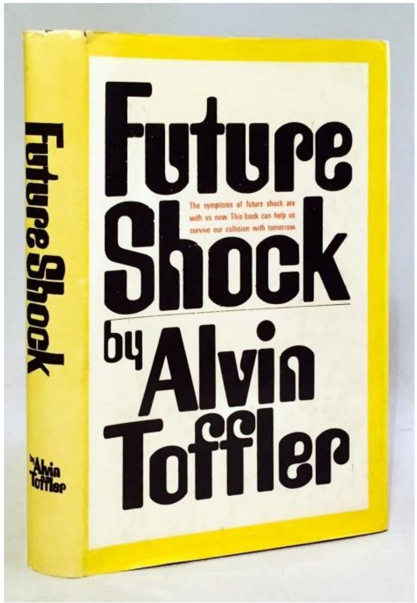
Future Shock

"The rate of change increases at an accelerating speed, without a corresponding acceleration in the rate at which responses can be made; and this brings us nearer the threshold beyond which control is lost."


Future Shock
by Alvin Toffler
The symptoms of future shock are with us now. This book can help us survive our collision with tomorrow.
Future Shock
by Alvin Toffler

Toffler, quoting Sir Geoffry Vickers, p396.

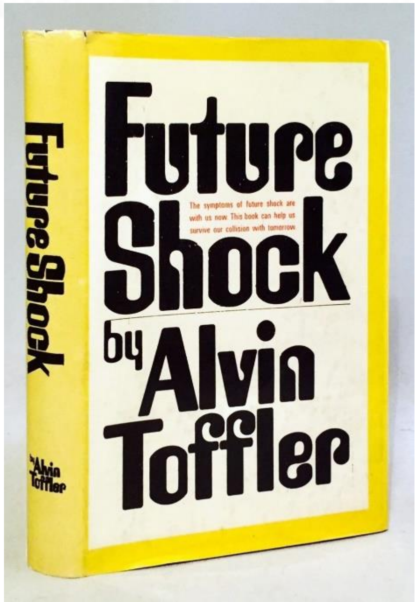
Future Shock


Future Shock
The symptoms of future shock are with us now. This book can help us survive our collision with tomorrow.
by Alvin Toffler

Toffler, quoting Sir Geoffry Vickers, p396.

Decelerate

“Capture control of the decelerative thrust.”


Future Shock
by Alvin Toffler
The symptoms of future shock are with us now. This book can help us survive our collision with tomorrow
Future Shock
by Alvin Toffler

Toffler, quoting Sir Geoffry Vickers, p396.

Decelerate:

“Capture Control of the Accelerative Thrust”

- Education PreK-12
- Toffler’s ideas…
- Winn’s work…

Decelerate:

“Capture Control of the Accelerative Thrust”

- Give defense the advantage over attackers at greatest scale and least cost
- Cybersecurity solutions with (mostly) positive knock-on effects
- Radical transparency to engage market forces
- Environmental model
  - Don’t pass the trash
  - Cap-and-trade, “polluter pays”
- Aim for stability, not overmatch and deterrence

Decelerate:

“Capture Control of the Accelerative Thrust”

- Full public policy panoply
  - Carrots, sticks, and sermons
- “Regulation” of technology
  - Software liability
  - GDPR
  - New models to monetize innovation

@Jason_Healey

THANK YOU