Insicurezze *e responsabilità*
nell'intersezione tra 'cyber and nuclear risk'

Scienza, ambiente, nucleare, guerra. Le implicazioni sistemiche del disarmo nucleare
Convegno sul disarmo nucleare a cura del coordinamento AGiTe

Centro Studi Sereno Regis
ricerca educazione azione per la pace l'ambiente la sostenibilità

Norberto Patrignani

Torino, 24 Settembre 02022

un po' di storia

1983: a Soviet satellite detected the launch of U.S. missiles

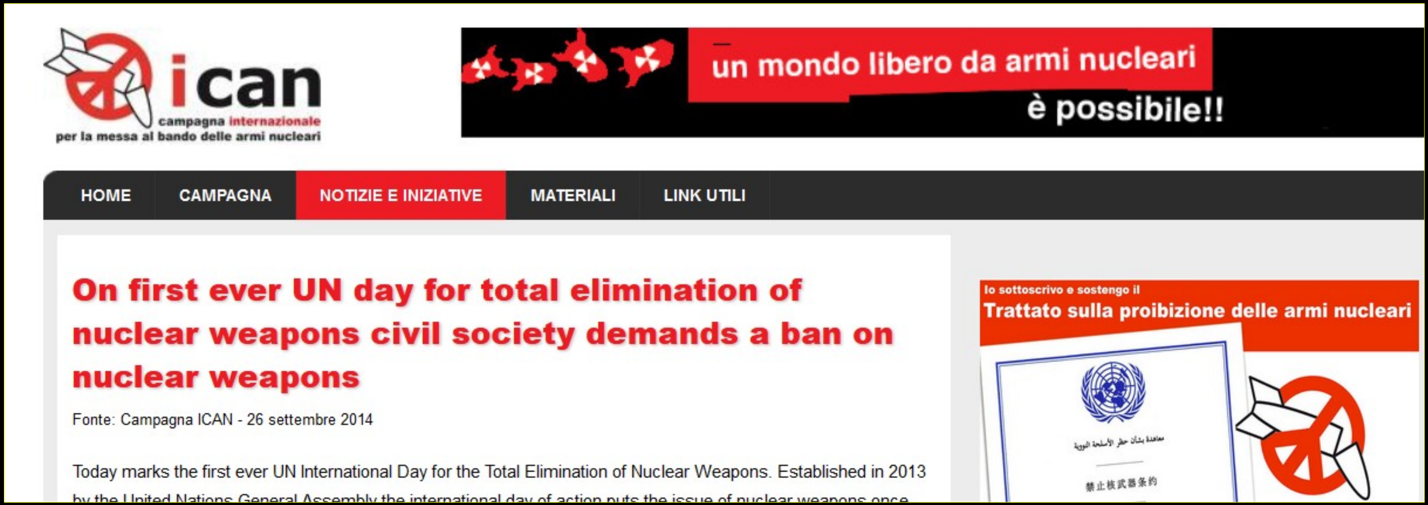
September 26, 1983, 00:14 (Moscow time)

Stanislav Petrov
(1939-2017)

Colonel Petrov had only minutes to decide whether the alarms going off in the middle of the night indicated the real thing, the beginning of World War III, or a false alarm.

Petrov, however, had his doubts.
..if the United States, which had thousands of nuclear weapons, was going to start a war, it would do it with more than just five missiles. Petrov told his superiors that it was a false alarm, even though he had no data at the time to confirm this.

Later investigations revealed that reflection of the sun on the tops of clouds had fooled the satellite into thinking it was detecting missile launches. While the Soviet system used an orbit designed to minimize the chances of false alarms, on that night, shortly after the autumn equinox, the early warning satellites, sun, and clouds aligned in such a way to maximize the sun's reflection.


ican
campagna internazionale
per la messa al bando delle armi nucleari
un mondo libero da armi nucleari
è possibile!!
HOME
CAMPAGNA
NOTIZIE E INIZIATIVE
MATERIALI
LINK UTILI
Io sottoscrivo e sostengo il
Trattato sulla proibizione delle armi nucleari
معاهدة بشأن حظر الأسلحة النووية
禁止核武器条约

On first ever UN day for total elimination of nuclear weapons civil society demands a ban on nuclear weapons

Fonte: Campagna ICAN - 26 settembre 2014

Today marks the first ever UN International Day for the Total Elimination of Nuclear Weapons. Established in 2013 by the United Nations General Assembly the international day of action puts the issue of nuclear weapons once

Source: MacDonald, E. (2015). *The Man Who Saved the World*. Union of Concerned Scientists

1939: Szilard

"*Spegnemmo tutto e tornammo a casa.*
Quella notte, nella mia mente non vi era il minimo dubbio
che il mondo era diretto verso un grande dolore"
Leo Szilard, 1939

dopo aver visto la prima reazione atomica a catena la notte del 3 Marzo 1939 (Klein, 1992).
Szilard firmò il "rapporto Franck", nel giugno 1945, insieme a importanti fisici del progetto Manhattan
per sconsigliare il governo degli Stati Uniti a usare la bomba atomica

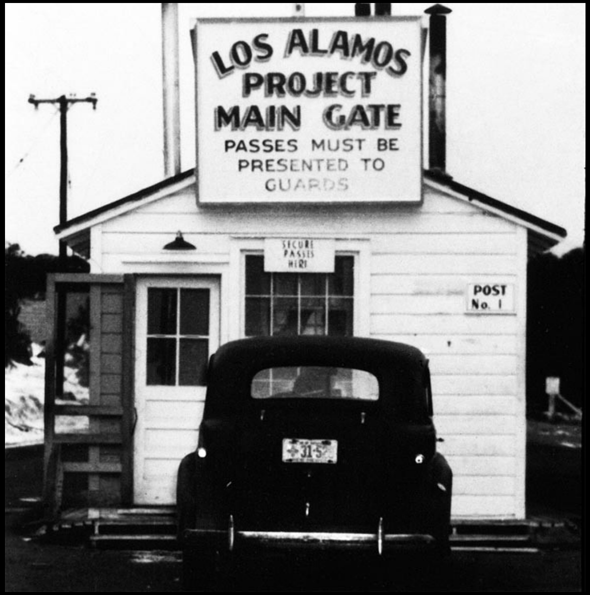
Leó Szilárd
(1898-1964)

La storia purtroppo confermò i presentimenti di Szilard e,
dopo il lancio della prima bomba atomica su Hiroshima,
il fisico Robert Oppenheimer scrisse: "*i fisici hanno conosciuto il peccato*".
Lo stesso rischio lo stanno correndo gli informatici.
Lo sviluppo di robot autonomi, dotati di armi letali,
sensori e sofisticati algoritmi di intelligenza artificiale
rischia di scatenare una nuova corsa agli armamenti in versione *cyberwar*,
spingendo gli scienziati dei computer e l'umanità intera verso
una soglia che forse non dovremmo attraversare

Patrignani, N. (2018, 11 Ottobre). *Perché vanno fermati i robot killer*. L'Adige.

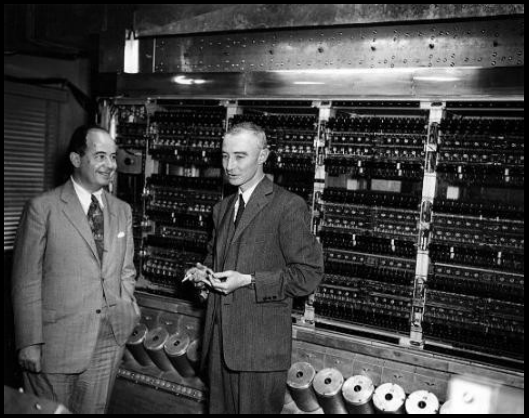
Source: Klein G. (1992), *The Atheist and the Holy City: Encounters and Reflections*, MIT Press.

1943: a machine for optimizing atomic bomb's effect



Los Alamos National Lab
(www.lanl.gov)

Early IBM machines that were used
at Los Alamos
(Atomic Heritage Foundation)

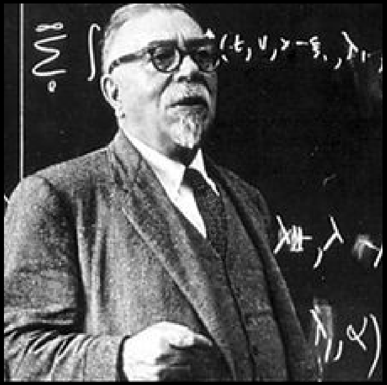


Princeton, 1952,
John Von Neumann,
Robert Oppenheimer

John Von Neumann
worked at Los Alamos on the mathematics of explosive shockwaves for the implosion-type "Fat Man" weapon.
He worked with IBM mechanical tabulating machines, tailored for this specific purpose.
As he grew familiar with the tabulators, he began to imagine a more general machine,
one that could handle far more general mathematical challenges: ***a computer***.

Source: www.lanl.gov

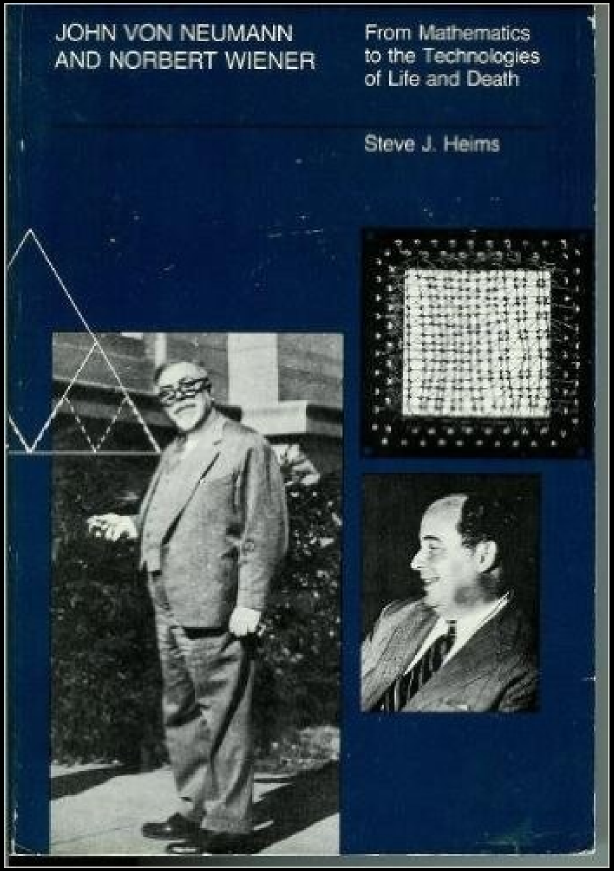
Norbert Wiener & John Von Neumann



Norbert Wiener
(1894-1964)

"I do not expect to publish any future work of mine which may do damage in the hands of irresponsible militarists..."

"A Scientist Rebels"
Atlantic Monthly, January, 1947



JOHN VON NEUMANN
AND NORBERT WIENER

From Mathematics
to the Technologies
of Life and Death

Steve J. Heims

John Von Neumann
(1903-1957)

"... I would prefer not to join the Board (of Bulletin of Atomic Scientists), since I have ... avoided all participation in public activities, which are not of a purely technical nature"

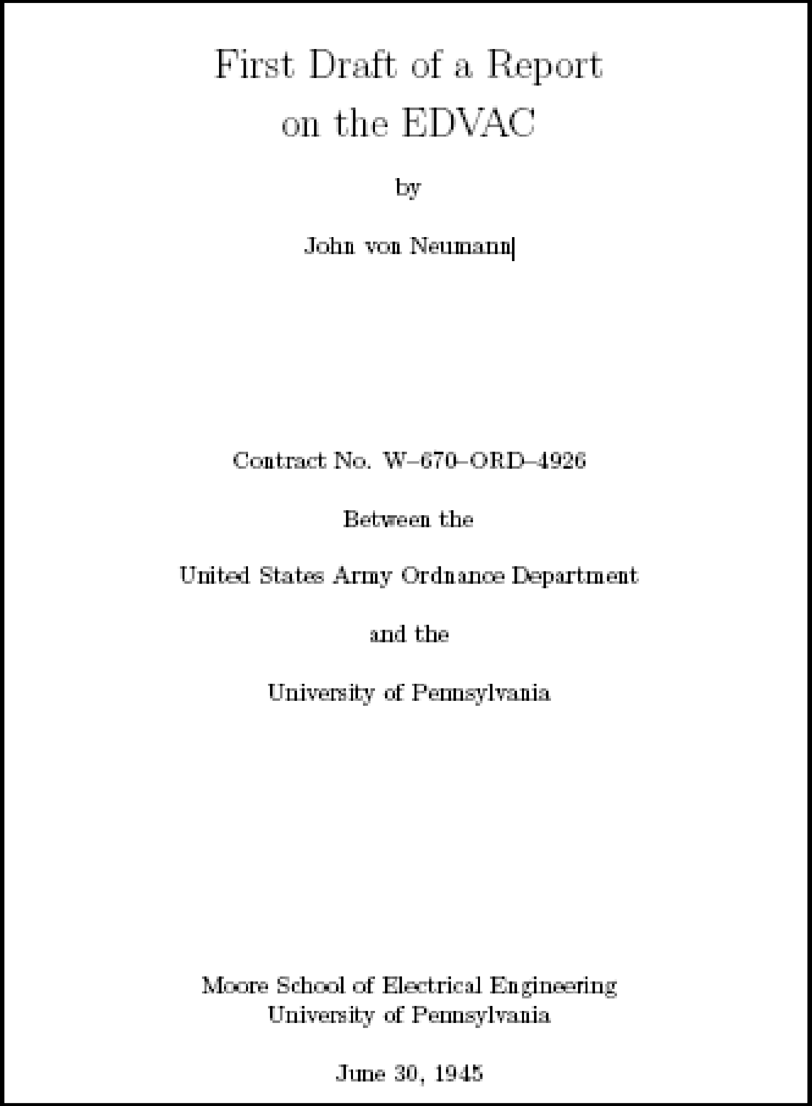
John Von Neumann to
Norman Cousins
(Library of Congress archives)
May 22, 1946

Source: Heims, S.J. - "John Von Neumann and Norbert Wiener, from mathematics to the technologies of life and death", MIT Press, Cambridge, MA, 1980

1945: Von Neumann Architecture

John Von Neumann
(1903-1957)

1944: EDVAC
University of Pennsylvania



First Draft of a Report
on the EDVAC

by

John von Neumann

Contract No. W–670–ORD–4926

Between the

United States Army Ordnance Department

and the

University of Pennsylvania

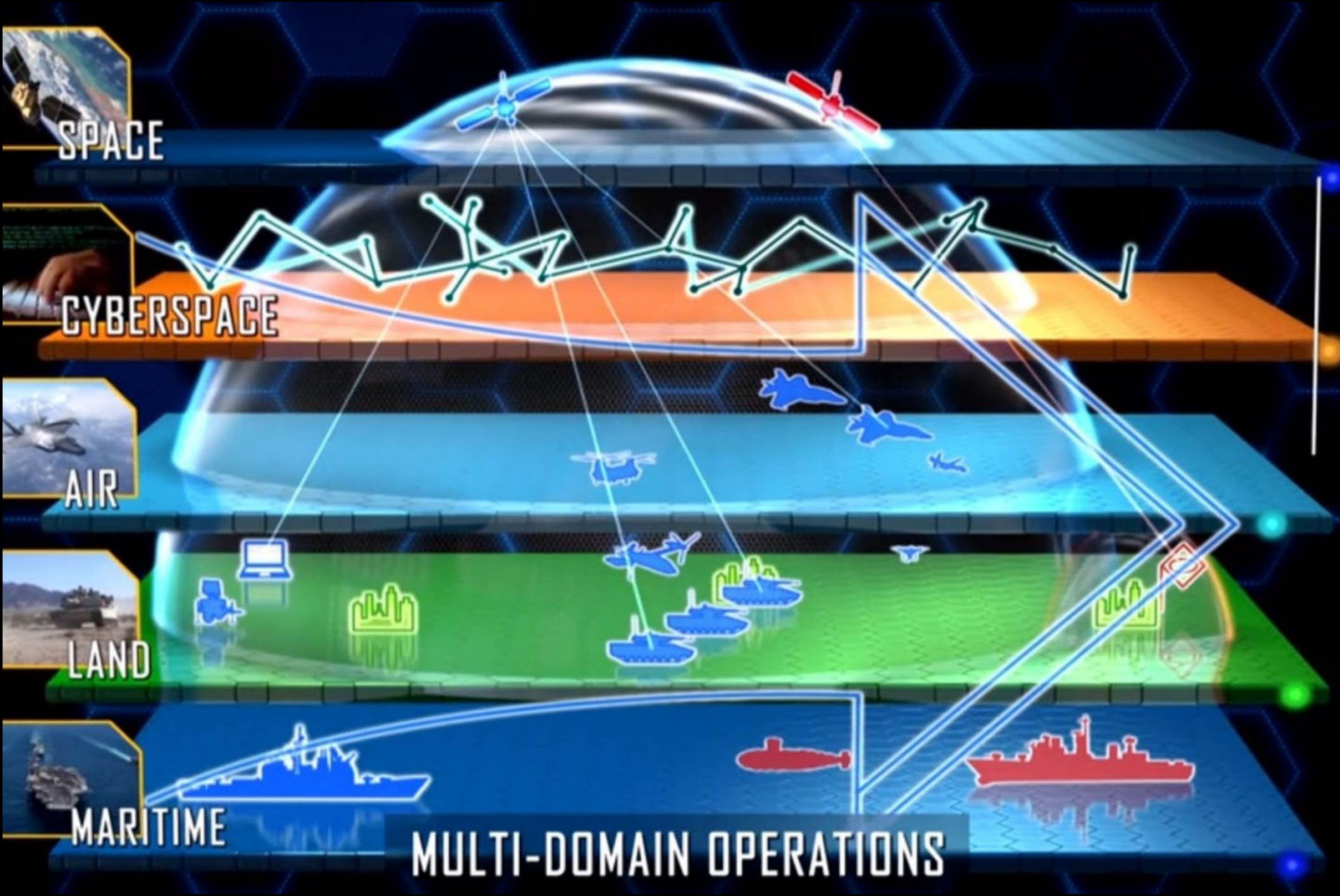
Moore School of Electrical Engineering
University of Pennsylvania

June 30, 1945

Also with contributions by
Herman Goldstine, John Mauchly, J. Presper Eckert, Arthur Burks

Source: "First Draft of a Report on the EDVAC", J.V.Neumann Moore School of Electrical Engineering, University of Pennsylvania, 1945 le armi nucleari sono connesse con i computer?

20XX: la guerra nel XXI secolo



Source: https://www.defencetalk.com

le armi nucleari

DOE (Department of Energy

NNSA (National Nuclear Security Administration)

NC3 (Nuclear Command Control Communication)

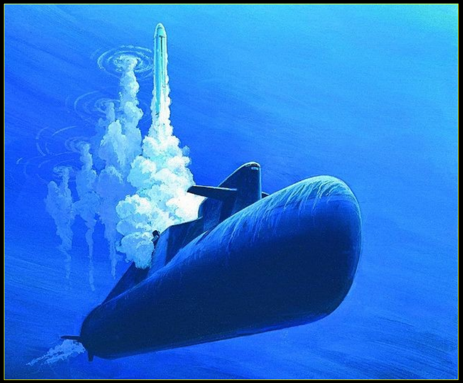
early warning system
satellites

cyber-risks
social engineering
cyber-attacks / supply-chain
bugs!

cyber-security
confidentiality
integrity
availability

ICBM
Intercontinental
Ballistic Missiles

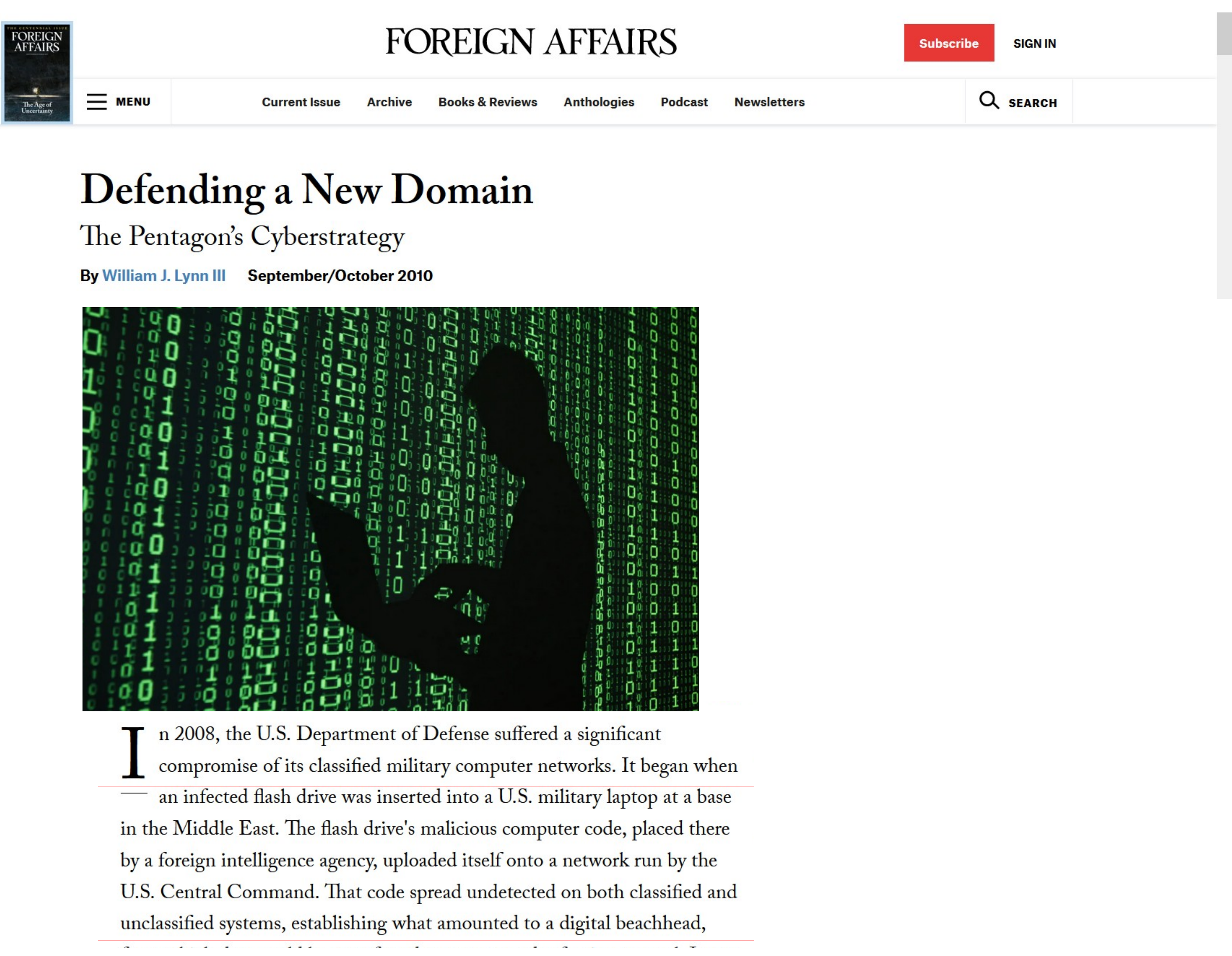
Air bombers
with gravity and cruise missiles



SLBM
Submarine-Launched
Ballistic Missiles

Source: Nuclear Posture Review 2018 - dod.defense.gov

2008: intrusion via social engineering (es.USB)



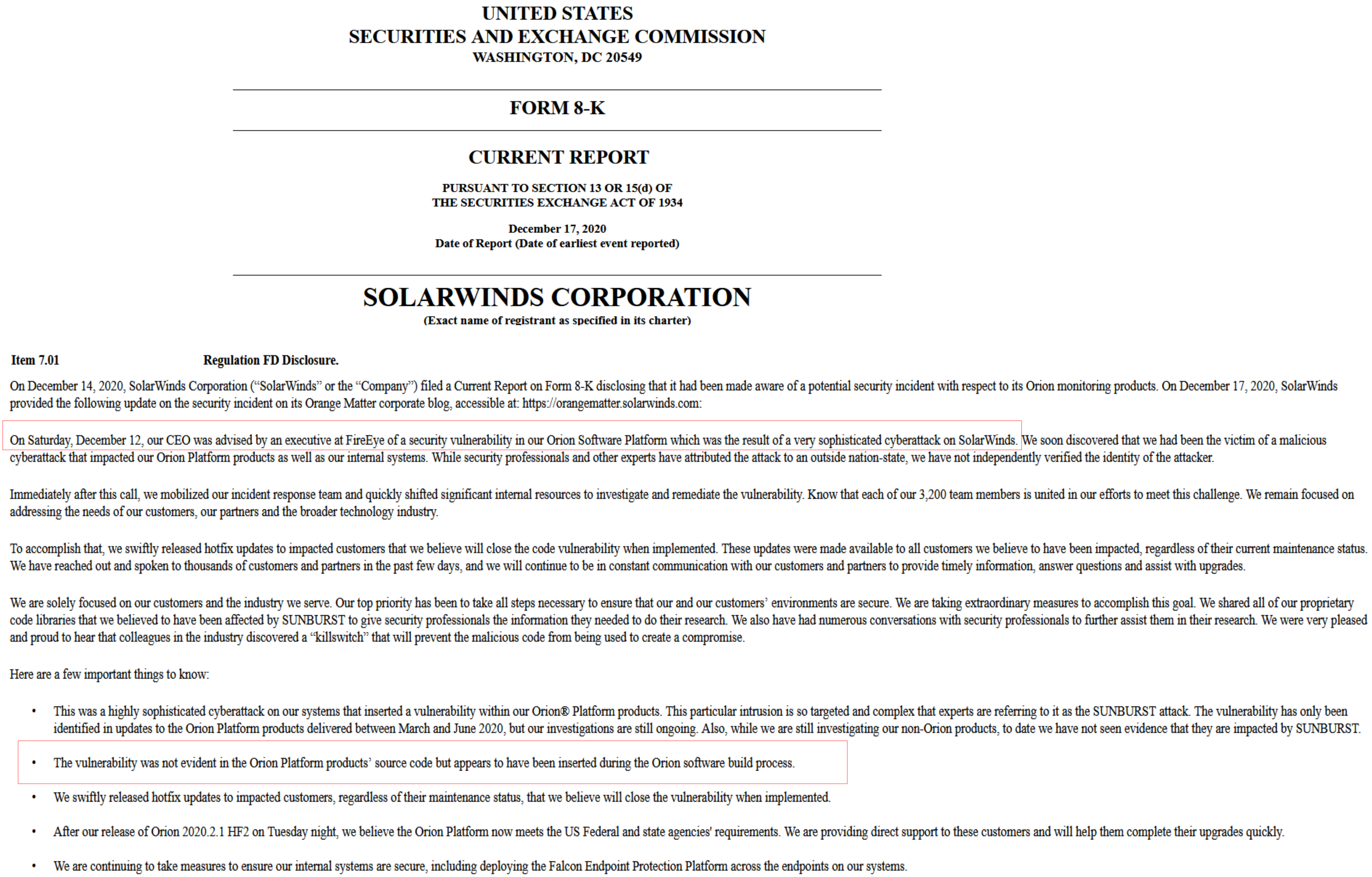
Defending a New Domain

The Pentagon's Cyberstrategy

By William J. Lynn III September/October 2010

In 2008, the U.S. Department of Defense suffered a significant compromise of its classified military computer networks. It began when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead,

2020: intrusion via supply-chain



UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, DC 20549

FORM 8-K

CURRENT REPORT

PURSUANT TO SECTION 13 OR 15(d) OF
THE SECURITIES EXCHANGE ACT OF 1934

December 17, 2020
Date of Report (Date of earliest event reported)

SOLARWINDS CORPORATION
(Exact name of registrant as specified in its charter)

Item 7.01 **Regulation FD Disclosure.**

On December 14, 2020, SolarWinds Corporation ("SolarWinds" or the "Company") filed a Current Report on Form 8-K disclosing that it had been made aware of a potential security incident with respect to its Orion monitoring products. On December 17, 2020, SolarWinds provided the following update on the security incident on its Orange Matter corporate blog, accessible at: https://orangematter.solarwinds.com:

On Saturday, December 12, our CEO was advised by an executive at FireEye of a security vulnerability in our Orion Software Platform which was the result of a very sophisticated cyberattack on SolarWinds. We soon discovered that we had been the victim of a malicious cyberattack that impacted our Orion Platform products as well as our internal systems. While security professionals and other experts have attributed the attack to an outside nation-state, we have not independently verified the identity of the attacker.

Immediately after this call, we mobilized our incident response team and quickly shifted significant internal resources to investigate and remediate the vulnerability. Know that each of our 3,200 team members is united in our efforts to meet this challenge. We remain focused on addressing the needs of our customers, our partners and the broader technology industry.

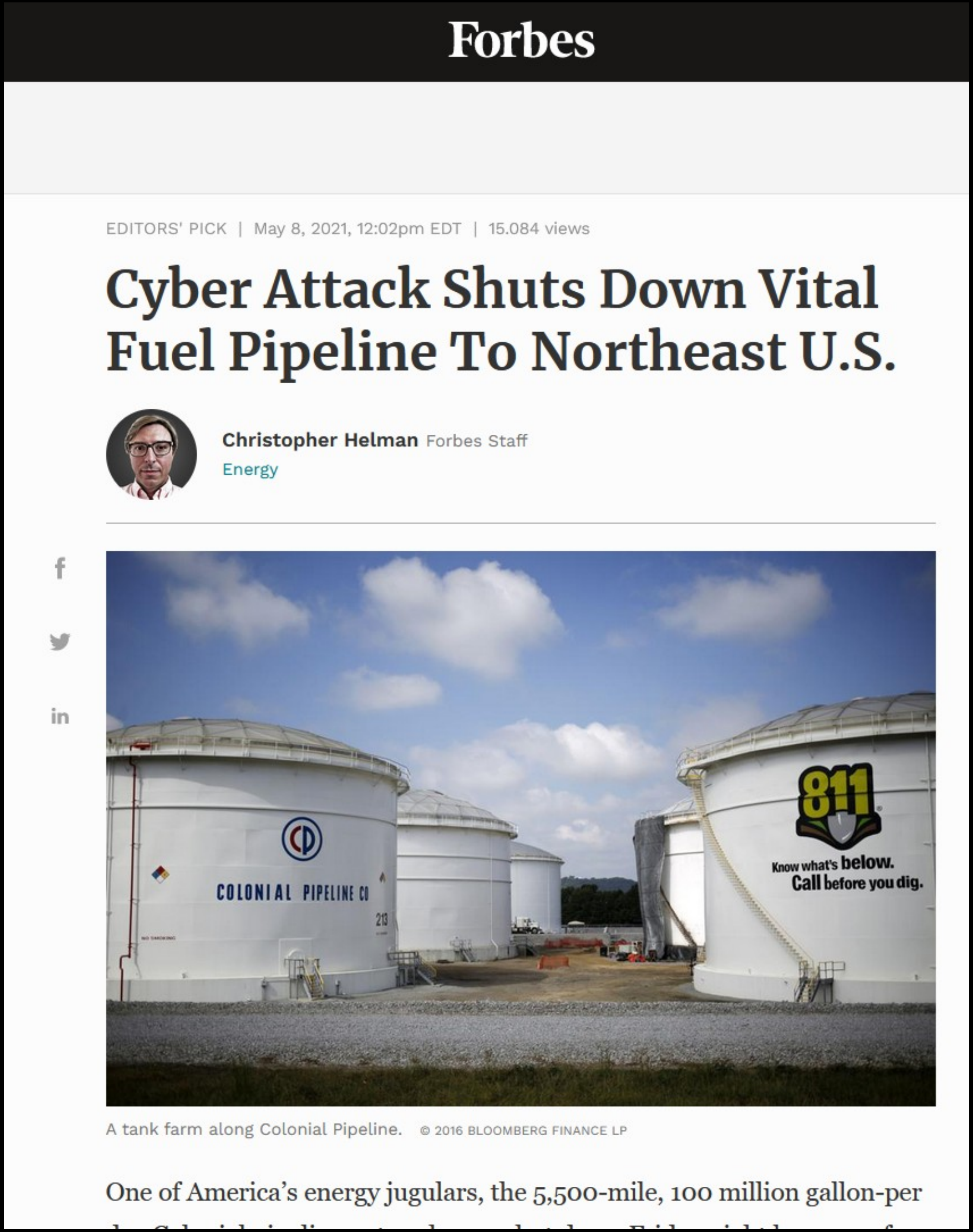
To accomplish that, we swiftly released hotfix updates to impacted customers that we believe will close the code vulnerability when implemented. These updates were made available to all customers we believe to have been impacted, regardless of their current maintenance status. We have reached out and spoken to thousands of customers and partners in the past few days, and we will continue to be in constant communication with our customers and partners to provide timely information, answer questions and assist with upgrades.

We are solely focused on our customers and the industry we serve. Our top priority has been to take all steps necessary to ensure that our and our customers' environments are secure. We are taking extraordinary measures to accomplish this goal. We shared all of our proprietary code libraries that we believed to have been affected by SUNBURST to give security professionals the information they needed to do their research. We also have had numerous conversations with security professionals to further assist them in their research. We were very pleased and proud to hear that colleagues in the industry discovered a "killswitch" that will prevent the malicious code from being used to create a compromise.

Here are a few important things to know:

- This was a highly sophisticated cyberattack on our systems that inserted a vulnerability within our Orion® Platform products. This particular intrusion is so targeted and complex that experts are referring to it as the SUNBURST attack. The vulnerability has only been identified in updates to the Orion Platform products delivered between March and June 2020, but our investigations are still ongoing. Also, while we are still investigating our non-Orion products, to date we have not seen evidence that they are impacted by SUNBURST.
- The vulnerability was not evident in the Orion Platform products' source code but appears to have been inserted during the Orion software build process.
- We swiftly released hotfix updates to impacted customers, regardless of their maintenance status, that we believe will close the vulnerability when implemented.
- After our release of Orion 2020.2.1 HF2 on Tuesday night, we believe the Orion Platform now meets the US Federal and state agencies' requirements. We are providing direct support to these customers and will help them complete their upgrades quickly.
- We are continuing to take measures to ensure our internal systems are secure, including deploying the Falcon Endpoint Protection Platform across the endpoints on our systems.

2021: intrusion via *cyber-attack*



EDITORS' PICK | May 8, 2021, 12:02pm EDT | 15.084 views

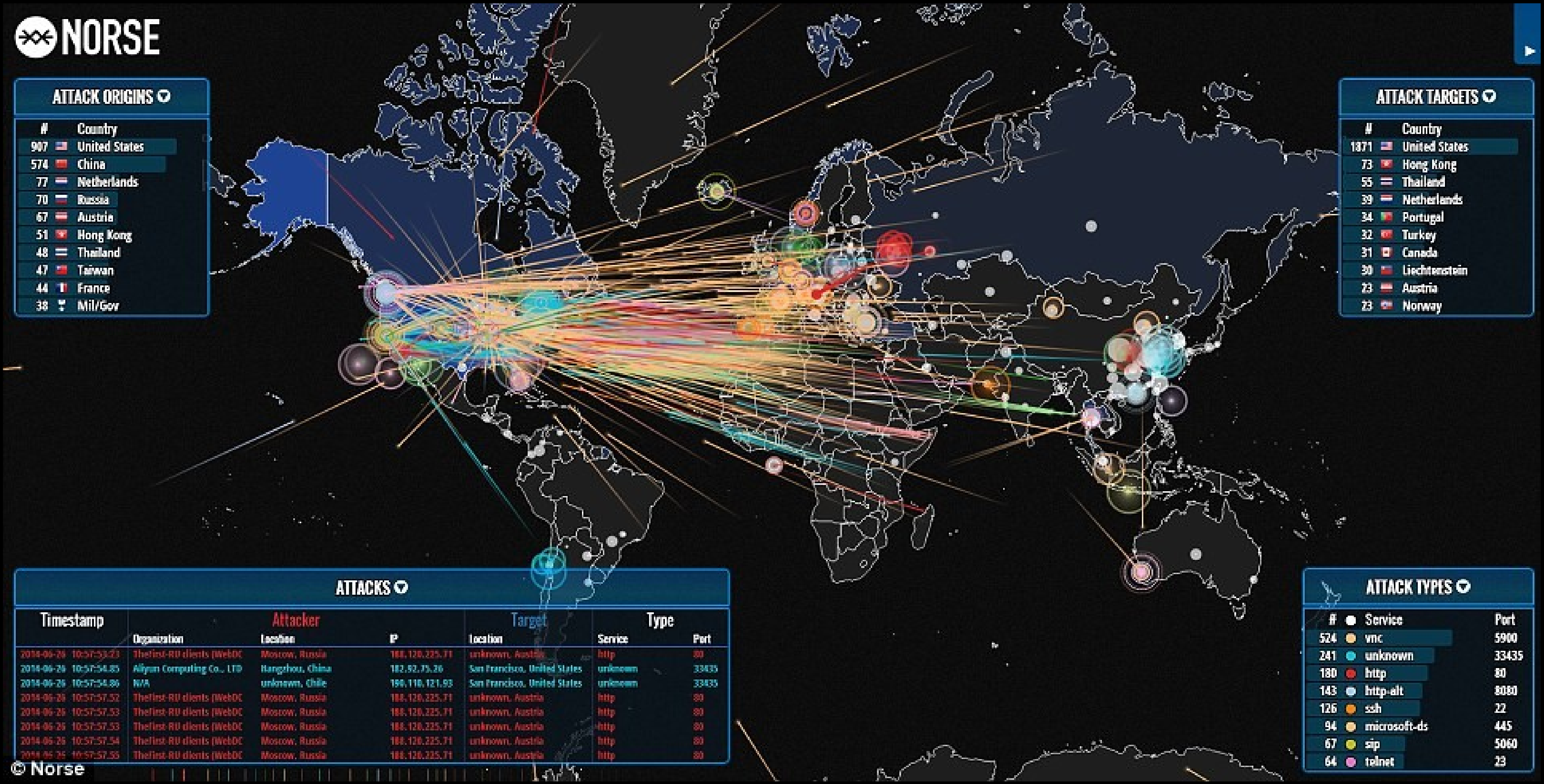
Cyber Attack Shuts Down Vital Fuel Pipeline To Northeast U.S.

Christopher Helman Forbes Staff
Energy

A tank farm along Colonial Pipeline. © 2016 BLOOMBERG FINANCE LP

One of America's energy jugulars, the 5,500-mile, 100 million gallon-per

daily *cyberwar*



NORSE

ATTACK ORIGINS

#	Country
907	United States
574	China
77	Netherlands
70	Russia
67	Austria
51	Hong Kong
48	Thailand
47	Taiwan
44	France
38	Mil/Gov

ATTACK TARGETS

#	Country
1871	United States
73	Hong Kong
55	Thailand
39	Netherlands
34	Portugal
32	Turkey
31	Canada
30	Liechtenstein
23	Austria
23	Norway

ATTACKS

Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-06-26 10:57:53.23	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:54.85	Aliyun Computing Co., LTD	Hangzhou, China	182.92.75.20	San Francisco, United States	unknown	33435
2014-06-26 10:57:54.86	N/A	unknown, Chile	190.110.121.93	San Francisco, United States	unknown	33435
2014-06-26 10:57:57.52	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.53	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.53	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.54	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.55	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80

ATTACK TYPES

#	●	Service	Port
524	●	vnc	5900
241	●	unknown	33435
180	●	http	80
143	●	http-alt	8080
126	●	ssh	22
94	●	microsoft-ds	445
67	●	sip	5060
64	●	telnet	23

© Norse

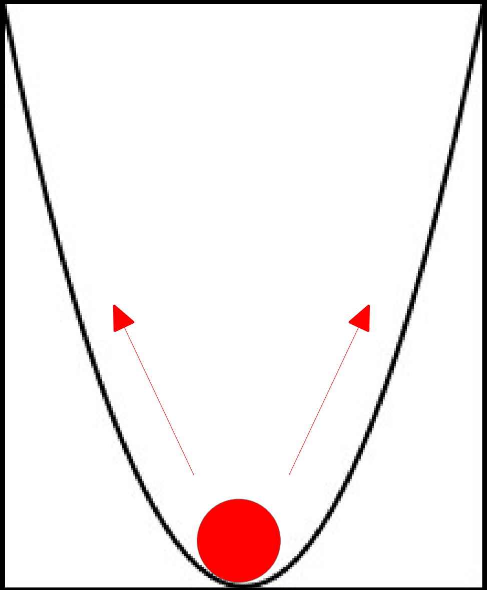
ogni giorno ci sono milioni di *cyber attack*: un *cyber attack* è un "*act of war*"?
perché i molti tentativi a livello UN di mettere al bando la *cyberwar* sono finora falliti?

Source: http://norsenet.com/resources/, https://www.pressenza.com/2021/04/why-the-u-s-shouldnt-play-games-with-cyberwarfare-as-its-power-declines perché i computer aumentano la vulnerabilità?

bugs! dai sistemi lineari ai sistemi a stati finiti

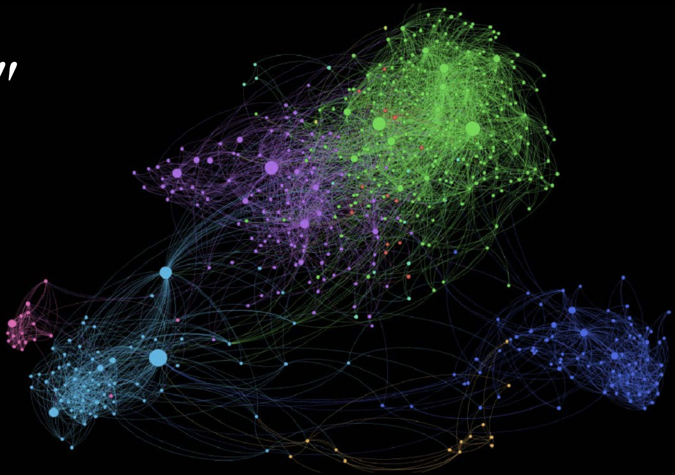
Sistemi Lineari
presupposto: bachi NON CI SONO
test: stress test verifica che non ci siano bachi

F < ϵ



Sistemi a Stati Finiti (software)
presupposto: bachi CI SONO
test: test "suite" verifica le "funzioni principali"

ϵ?



bugs! the limits of software testing

Edsger W. Dijkstra
(1930-2002)

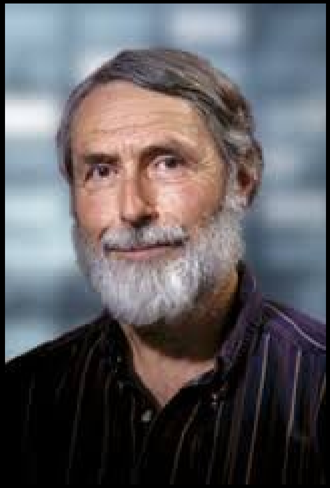
"*Program testing*
can be used
to show the presence of bugs,
but never
to show their absence"

Edsger W. Dijkstra (1972)
Computer Scientist
Winner of Turing Award (1972)

Dijkstra Algorithms, Structured Programming, Semaphores and against GOTO

Source: E.W.Dijkstra, "Notes On Structured Programming", Tech.University of Eindhoven, The Netherlands,1972

<u>bugs!</u> what can we (computer scientists/professionals) do?



Peter G.Neumann

"What are the intrinsic limitations
as to what can and cannot be guaranteed?
Nothing can be absolutely guaranteed.
There are always possibilities for undetected exceptions.
We can always do better, but cannot be perfect.
<u>It is desirable to design systems</u>
***<u>so that if something undesirable does happen</u>**,*
*it may be possible to **<u>contain it</u>***
in some sense relevant to the problem,
*or to **<u>undo it</u>**, or to **<u>compensate for it</u>**."*

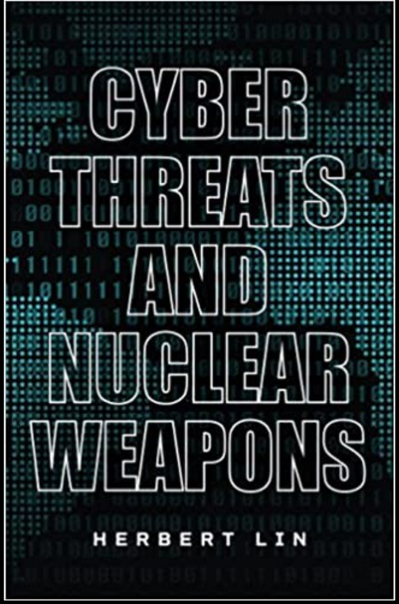
Peter G.Neumann
Computer Security and Human Values

bugs! what can we (computer scientists/professionals) do?

> *"Design the systems in such a way that*
> ***the role of software is not too much critical****;*
> *Software Reliability Requirement*
> *should be* ***reduced*** *at a level so low*
> *that can it be demonstrated and tested*
> *BEFORE the system is installed and switched on."*
> B.Littlewood, L.Strigini, 1993

Source: B.Littlewood, L.Strigini, "I rischi del software", Le Scienze, n.293, Gen 1993

2021: cyberthreats and nuclear weapons



1. computers' unreliability

- much of such technology now controlling US nuclear weapons was produced before the rise of the Internet
- cyber vulnerabilities have to do with flaws in the implementation or the design of a computer system that may be connected or controlling a missile or a nuclear weapon
- these are flaws in the design or implementation that if the bad guys know about them, they can make the system do something that the designers of the system never intended
- the first kind of risk: the fact that you have more computer systems out there and then you can be more likely to be hacked
- vulnerabilities are inherent in computer systems...
- the more and more we develop and deploy the complicated stuff, the more vulnerable we are
- **don't computerize unnecessarily**

2. cyberspace's unknown dynamics

- there's a different kind of cyber risk that comes about because of the potential for inadvertent or accidental escalation
- for example, an adversary's cyberattack may be intended to degrade our conventional forces, but we may think the adversary is going after our nuclear forces, ...so now they launched a cyberattack against one of the early warning satellites, and we see it
- are we to conclude that their intention is to compromise the tactical ballistic missile warning function, or the strategic ICBM warning function? if they start attacking our early warning satellites, we may misinterpret it
- if you are going to launch a cyberattack on an adversary, you might want to consider what the adversary might think about it
- time pressure makes understanding what's happening in cyberspace much more difficult
- be careful about how your actions in cyberspace will be perceived by others
- this points to reduction in the risk of inadvertent escalation and consequences
- **eliminating the ICBM force** would also significantly reduce cyber risk because you would lose the launch-on-warning time pressure

scenario 6: false
social media messaging
provoking war!

Source: Mecklin, J. (2021, 30 November). Interview: Stanford's Herbert Lin on "Cyber Threats and Nuclear Weapons", Bulletin of the Atomic Scientists

2021: cyberthreats and nuclear weapons

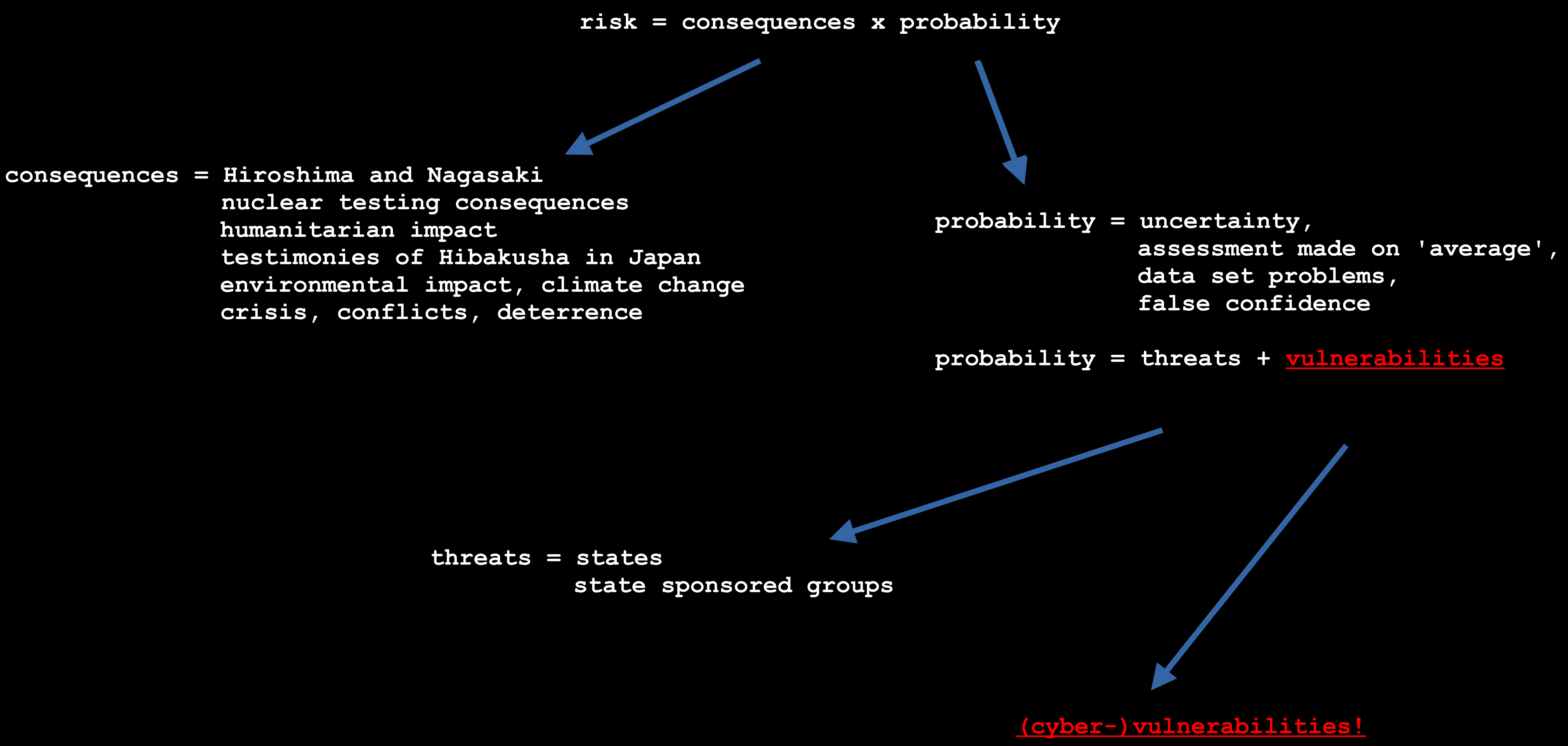
+ complessità

- sicurezza

"… everybody wants their information technology system to do more,
to have more functionality in some way. We want it to be better, faster, easier to use,
have more functions, support more applications…
The problem is that whenever you want a computer system to do more,
you have to make a bigger system…
And every computer professional will acknowledge that complexity is the enemy of security.
More complexity means less security."

Source: Mecklin, J. (2021, 30 November). Interview: Stanford's Herbert Lin on "Cyber Threats and Nuclear Weapons", Bulletin of the Atomic Scientists

2021: *cyberwar?*



risk = consequences x probability

consequences = Hiroshima and Nagasaki
nuclear testing consequences
humanitarian impact
testimonies of Hibakusha in Japan
environmental impact, climate change
crisis, conflicts, deterrence

probability = uncertainty,
assessment made on 'average',
data set problems,
false confidence

probability = threats + vulnerabilities

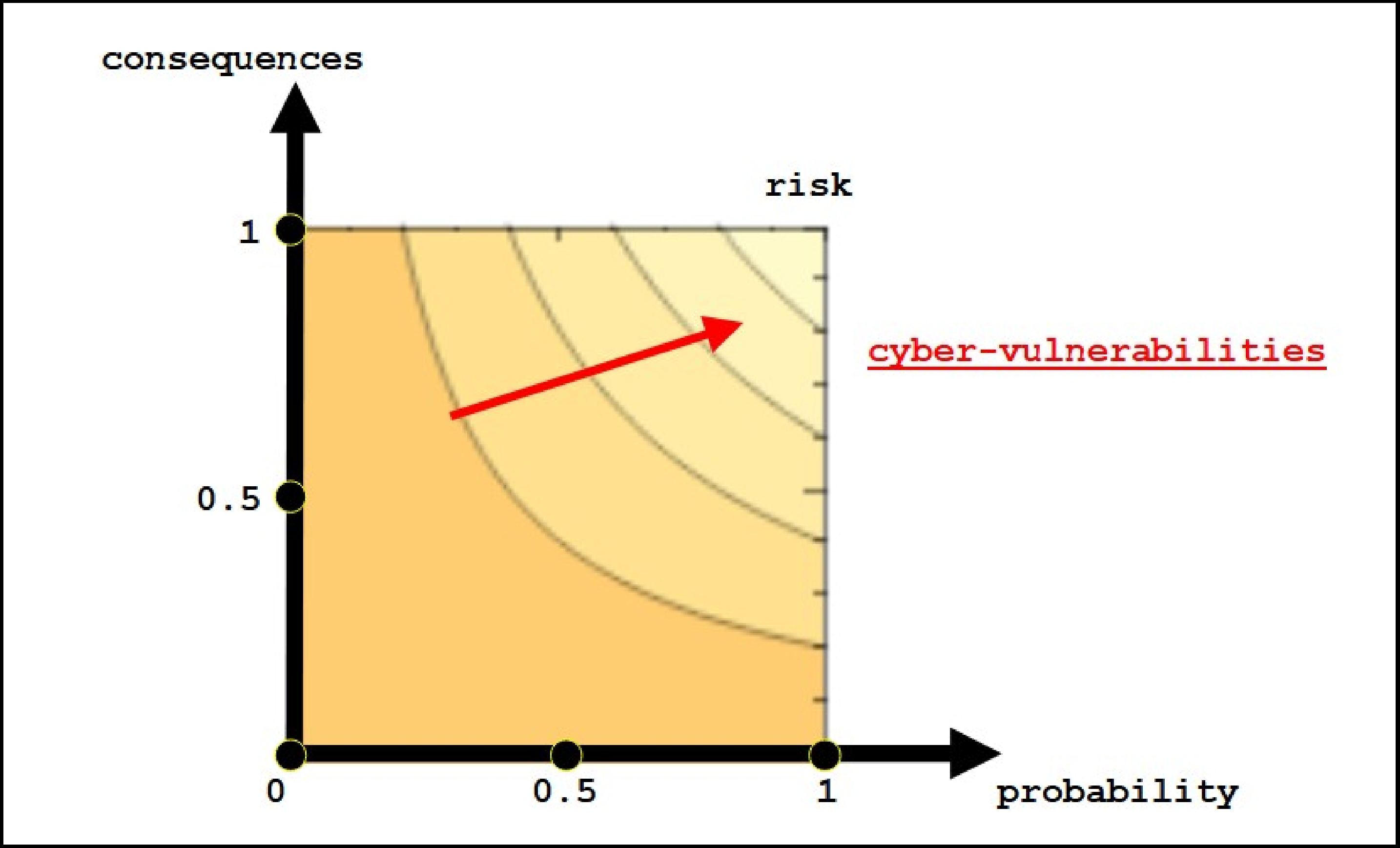
threats = states
state sponsored groups

(cyber-)vulnerabilities!

Source: adapted from Beyza Unal, Strategic Stability and Cyber and Space Dependency in Nuclear Assets, Chatham House (UK), 2021

2021: *cyberwar?*

cyber attack?
attribution?
response?



(cyber-)vulnerabilities = increased connectivity of networked systems
software & hardware vulnerability
supply-chain vulnerability
design vulnerability
tactical data links
server and facilities of missiles host countries

Source: adapted from Beyza Unal, Strategic Stability and Cyber and Space Dependency in Nuclear Assets, Chatham House (UK), 2021

"... the only thing more frightening than nuclear weapons is the thought of those weapons being connected to modern software systems"

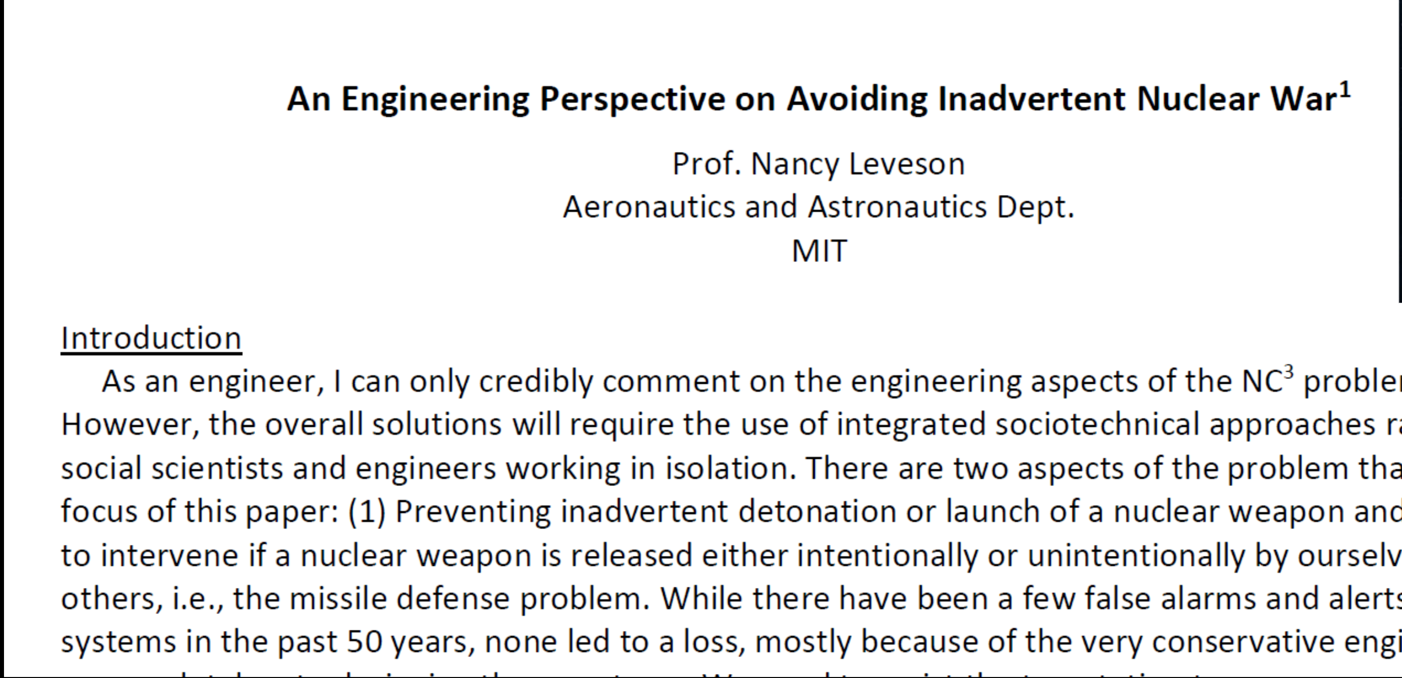
Jim Waldo, 2021

Distinguished Software Engineer
Sun Microsystems Laboratories

che fare?

2019: avoid software and complex designs *to prevent accidental detonation of nuclear weapons*

Nancy Leveson
MIT

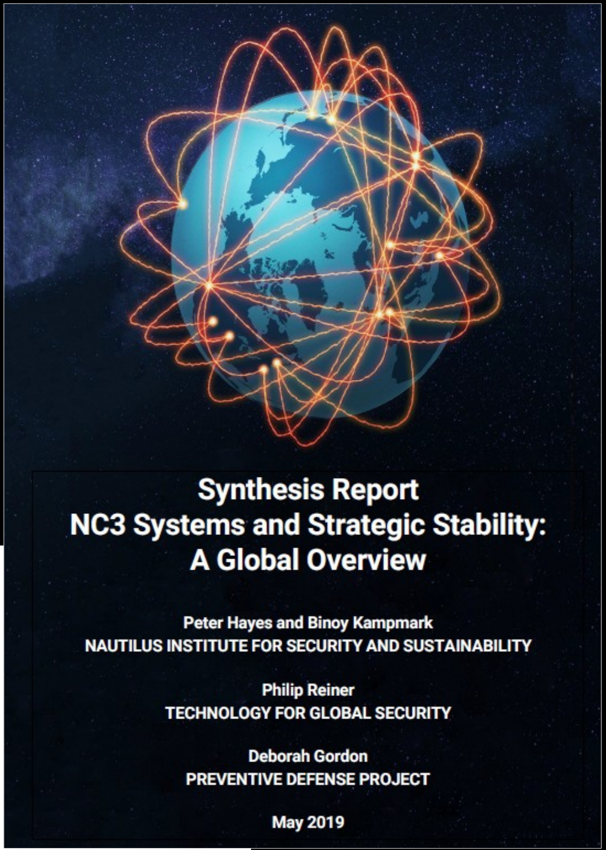


An Engineering Perspective on Avoiding Inadvertent Nuclear War[1]

Prof. Nancy Leveson
Aeronautics and Astronautics Dept.
MIT

Introduction

As an engineer, I can only credibly comment on the engineering aspects of the NC^3 problem. However, the overall solutions will require the use of integrated sociotechnical approaches rather than social scientists and engineers working in isolation. There are two aspects of the problem that are the focus of this paper: (1) Preventing inadvertent detonation or launch of a nuclear weapon and (2) ability to intervene if a nuclear weapon is released either intentionally or unintentionally by ourselves or others, i.e., the missile defense problem. While there have been a few false alarms and alerts in NC^3 systems in the past 50 years, none led to a loss, mostly because of the very conservative engineering



Synthesis Report
NC3 Systems and Strategic Stability:
A Global Overview

Peter Hayes and Binoy Kampmark
NAUTILUS INSTITUTE FOR SECURITY AND SUSTAINABILITY

Philip Reiner
TECHNOLOGY FOR GLOBAL SECURITY

Deborah Gordon
PREVENTIVE DEFENSE PROJECT

May 2019

Source: Leveson, N. (2019). An engineering perspective on avoiding inadvertent nuclear war, NAPSNet special reports July 25, 2019

2020: Pugwash on *cyberwar*

cyberwar and critical infrastructures

- when a *cyber-attack* should be considered as a “use of force” or as an “armed attack”?

- prohibit *cyber attacks* on critical infrastructures, nuclear installations and facilities

- develop an agreed list of critical infrastructures to be out-of-bounds for *cyber attacks*

- *cyber arms* control, development of P-5 work/statement on “Cyber and Nuclear Forces”

- understand *cyber vulnerabilities of nuclear weapon systems* and the risk of accidental use of nuclear weapons

- understand the dual-use character of *cyber technologies*, international arms export and arms control regulations

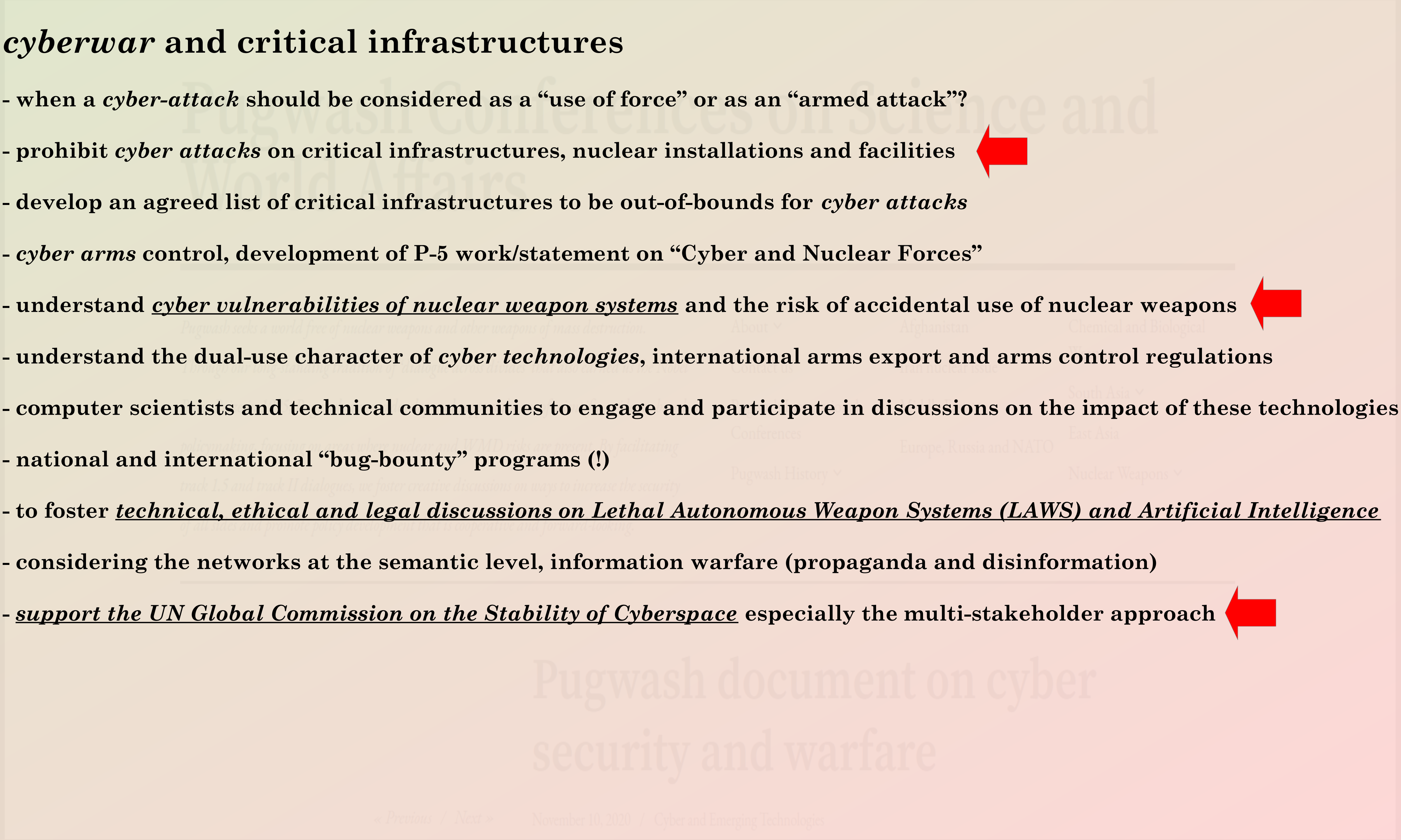
- computer scientists and technical communities to engage and participate in discussions on the impact of these technologies

- national and international “bug-bounty” programs (!)

- to foster *technical, ethical and legal discussions on Lethal Autonomous Weapon Systems (LAWS) and Artificial Intelligence*

- considering the networks at the semantic level, information warfare (propaganda and disinformation)

- *support the UN Global Commission on the Stability of Cyberspace* especially the multi-stakeholder approach



Pugwash Conferences on Science and World Affairs

Pugwash seeks a world free of nuclear weapons and other weapons of mass destruction.

policymaking, focusing on areas where nuclear and WMD risks are present. By facilitating

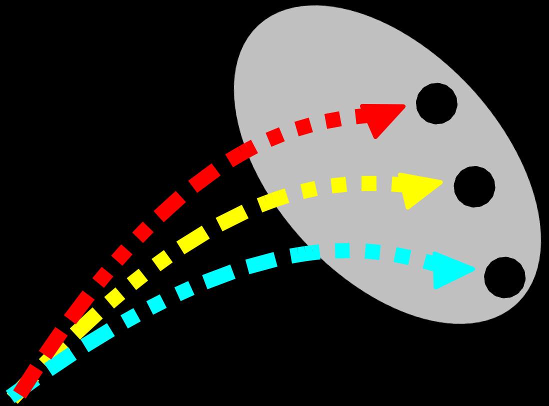
track 1.5 and track II dialogues, we foster creative discussions on ways to increase the security

of all sides and promote policy development that is cooperative and forward-looking.

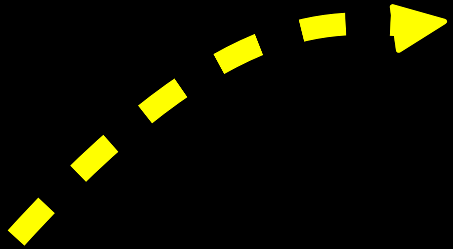
Pugwash document on cyber security and warfare

« Previous / Next » November 10, 2020 / Cyber and Emerging Technologies

evitare l'*epistemological shift*



- forecast, pre-***<u>vedere</u>*** =
    - fore+cast,
      to estimate how something will be in the future
    - *prae* (avanti) *videre* (vedere), vedere prima
      (soprattutto con gli occhi della mente)



- prediction, pre-***<u>dire</u>*** =
    - prophecy, to pronounce solemnly,
      a statement of what will happen in the future
    - *prae* (avanti) *dicere* (dire), annunciare che una cosa futura avverrà

- prescription, pre-***<u>scrivere</u>*** =
    - order, direction, written directions from a doctor
    - *prae* (avanti) *scribere* (scrivere), ordinare, comandare per iscritto,
      ordine del medico

Fonte: Wikimedia Commons - Francisco de Goya (1746–1828), Il sonno della ragione produce mostri

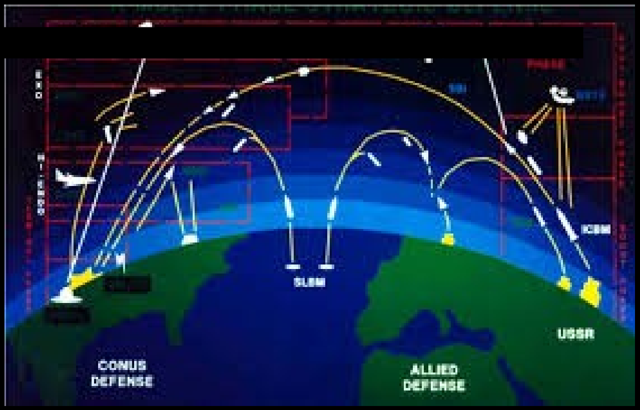
1995: SDI Report, prof.David Parnas

Ethical Dilemmas for Computer Professionals

SDI Report

"... Software is released for use,
***not** when it is known to be correct,*
*but when the **rate of discovering new errors***
slows down to one
*that management considers **acceptable**.*
*... Because of the **extreme demands on the system***
and our inability to test it,
we will never be able to believe,
with any confidence,
that we have succeeded."

Prof.D.Parnas, 1995



Source: "Why the SDI software system will be untrustworthy", D.Parnas, University of Victoria, 26 June 1995
SDI = Strategic Defense Initiative, also known as 'Star Wars'

2020: IFIP Code of Ethics and Professional Condict

- 2020: adozione da parte dell'IFIP (International Federation for Information Processing) del ACM "Code of Ethics and Professional Conduct"

- necessità di andare oltre le competenze tecniche
    - per aiutare a minimizzare i rischi e gli errori non intenzionali ("good-guys"!)
    - per guidare i progetti verso un contributo positivo alla società e al pianeta

- nel preambolo è scritto:

"*le attività delle persone definite 'computer professional' cambiano il mondo. Per agire responsabilmente, esse devono riflettere sugli impatti più ampi del loro lavoro, supportando sempre il bene pubblico*" (IFIP, 2021)

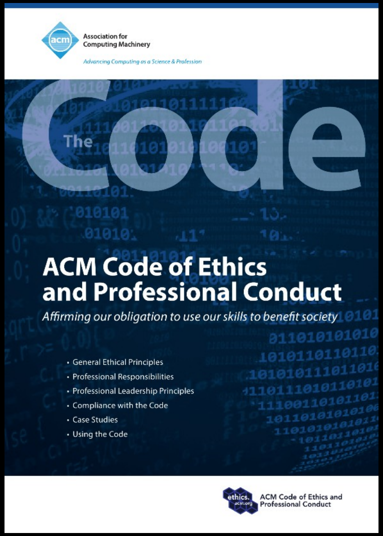
- priorità al "public interest"
- anticipare gli impatti sociali e ambientali ("*avoid harms*")

… take special care of systems that become integrated into the infrastructure of society…

… report any signs of system risks that might result in harm.

- recuperare un'etica della responsabilità,

un'etica per la civiltà tecnologica (Jonas, 1979)



Association for Computing Machinery

Advancing Computing as a Science & Profession

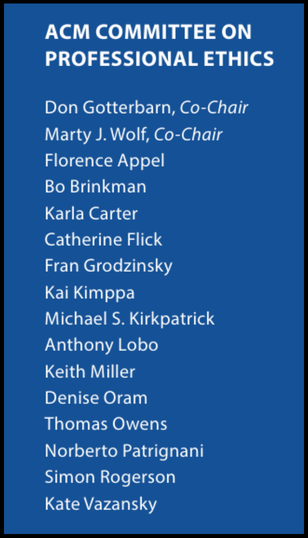
The Code

ACM Code of Ethics and Professional Conduct

Affirming our obligation to use our skills to benefit society

- General Ethical Principles
- Professional Responsibilities
- Professional Leadership Principles
- Compliance with the Code
- Case Studies
- Using the Code

ACM Code of Ethics and Professional Conduct

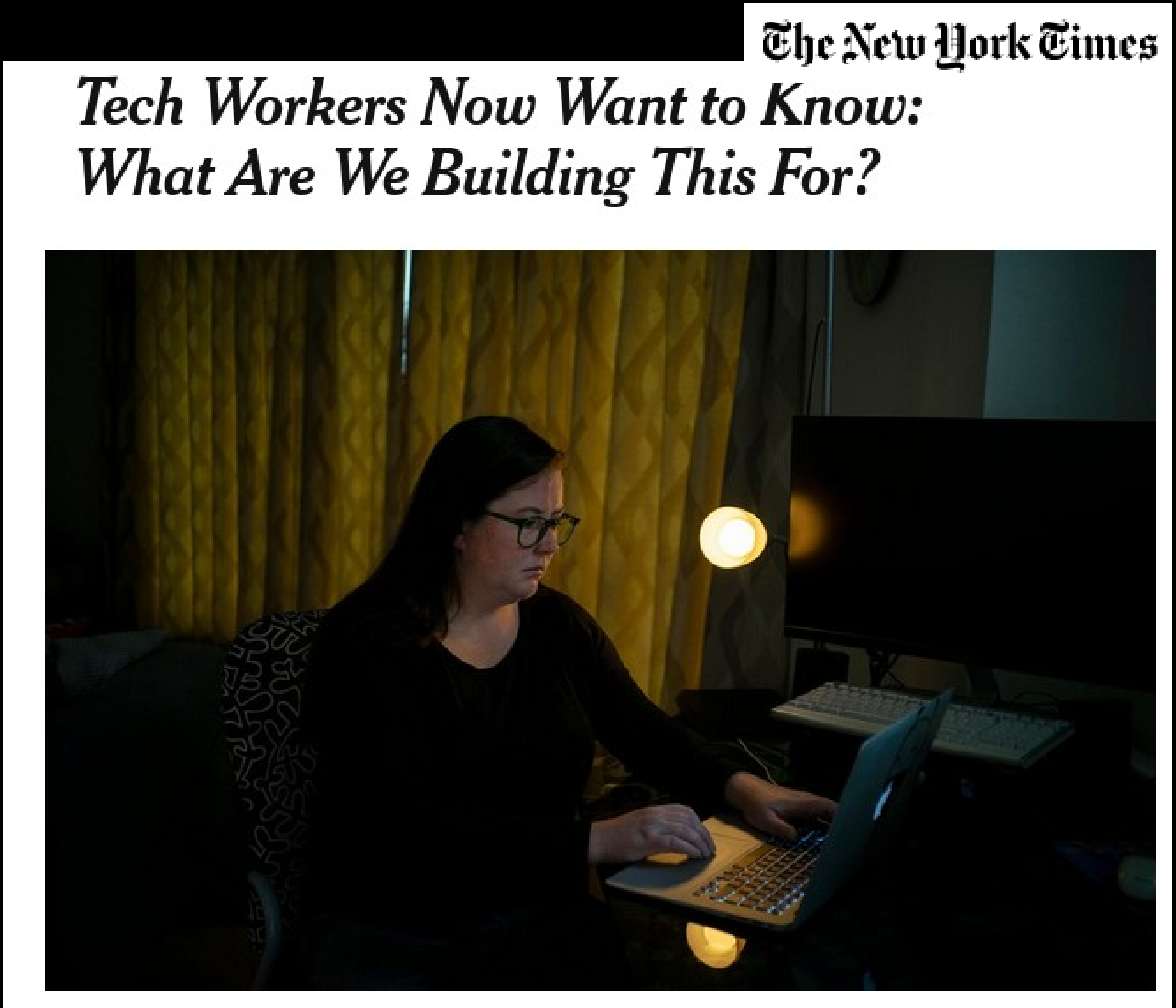


ACM COMMITTEE ON PROFESSIONAL ETHICS

Don Gotterbarn, *Co-Chair*
Marty J. Wolf, *Co-Chair*
Florence Appel
Bo Brinkman
Karla Carter
Catherine Flick
Fran Grodzinsky
Kai Kimppa
Michael S. Kirkpatrick
Anthony Lobo
Keith Miller
Denise Oram
Thomas Owens
Norberto Patrignani
Simon Rogerson
Kate Vazansky

2018: Big Tech Workers

Laura Nolan,
a software engineer
left Google in June 2018
over the company's
involvement
in Project Maven,
an effort to build
artificial intelligence
for the
Department of Defense



The New York Times

Tech Workers Now Want to Know: What Are We Building This For?

Credit CreditPaulo Nunes dos Santos for The New York Times

Source: Kate Conger and Cade Metz, The New York Times, Oct. 7, 2018

nel nostro tempo,
come persone esperte di informatica,
o *computer professionals*,
dobbiamo assumerci la responsabilità di dire
cosa può essere e
cosa non può essere automatizzato

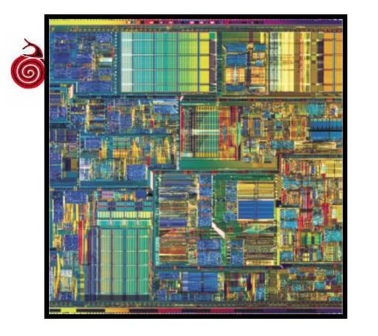
proposta: non chiamiamola "intelligenza artificiale",
parliamo di "algoritmi dinamici"
che si "calibrano" con (tanti) dati

le tecnologie dell'informazione
sono arrivate a plasmare
la società e il pianeta in modo inquietante,
sono parte integrante delle sfide dell'*Antropocene*

per affrontare queste sfide
la filiera del dato-informazione-conoscenza
deve passare ad una visione sistemica dell'*infosfera*
sviluppando tecnologie
socialmente desiderabili,
ambientalmente sostenibili e
eticamente accettabili

Fonte: Patrignani, N. (2020). Teaching Computer Ethics: Steps towards Slow Tech, a Good, Clean, and Fair ICT. Uppsala University. download URN: urn:nbn:se:uu:diva-403686

Slow Tech



una "*bussola euristica*"

mostra NON SOLO l'attuale direzione, ma anche nuove possibilita'! ("funzione euristica")

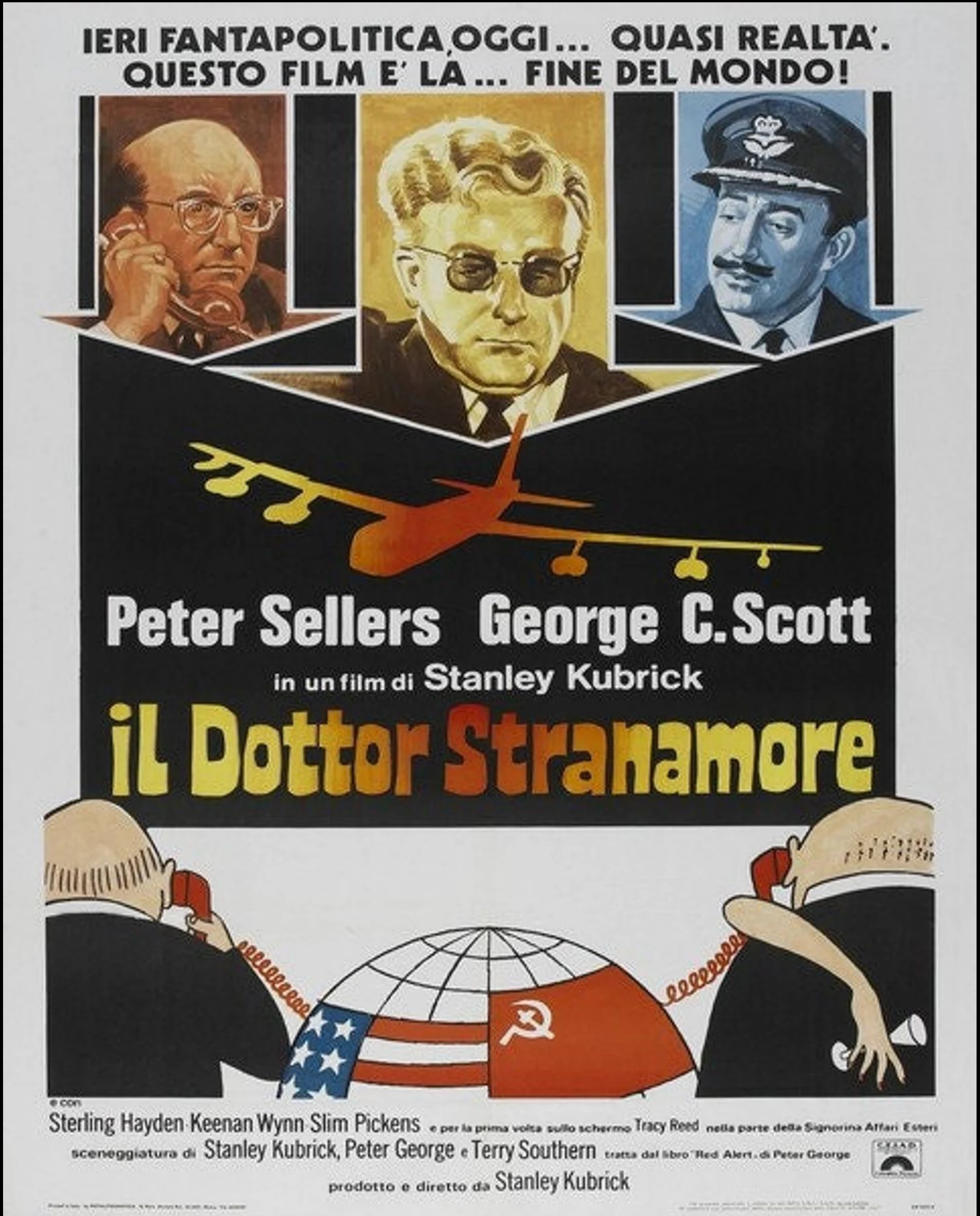
- per la progettazione di sistemi digitali basati su un'informatica *buona, pulita e giusta*

- basata sul concetto di LIMITI (del pianeta e degli esseri umani) (e una critica della precedente assunzione che l'ICT continuera' a crescere esponenzialmente, sempre più veloce, ... "no limits")

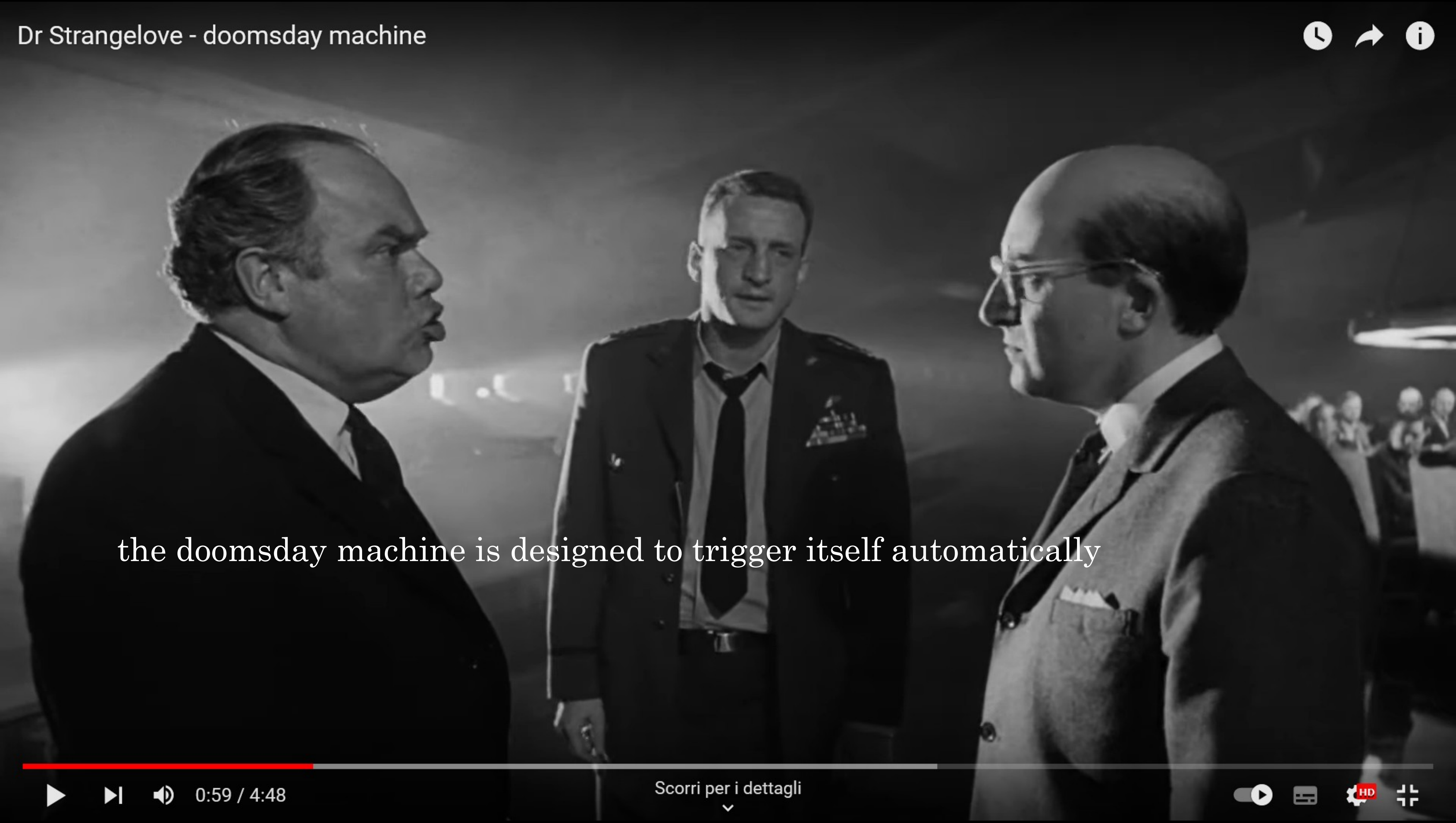
- basata sull'analisi trasparente della rete degli stakeholders (senza ignorare i conflitti, le diverse visioni, stimolando una riflessione etica)

Source: Patrignani, N. (2020). Teaching Computer Ethics: Steps towards Slow Tech, a Good, Clean, and Fair ICT. Uppsala University

conclusioni


IERI FANTAPOLITICA, OGGI... QUASI REALTA'.
QUESTO FILM E' LA... FINE DEL MONDO!
Peter Sellers George C. Scott
in un film di Stanley Kubrick
il Dottor Stranamore
e con
Sterling Hayden · Keenan Wynn · Slim Pickens e per la prima volta sullo schermo Tracy Reed nella parte della Signorina Affari Esteri
sceneggiatura di Stanley Kubrick, Peter George e Terry Southern tratta dal libro "Red Alert" di Peter George
prodotto e diretto da Stanley Kubrick

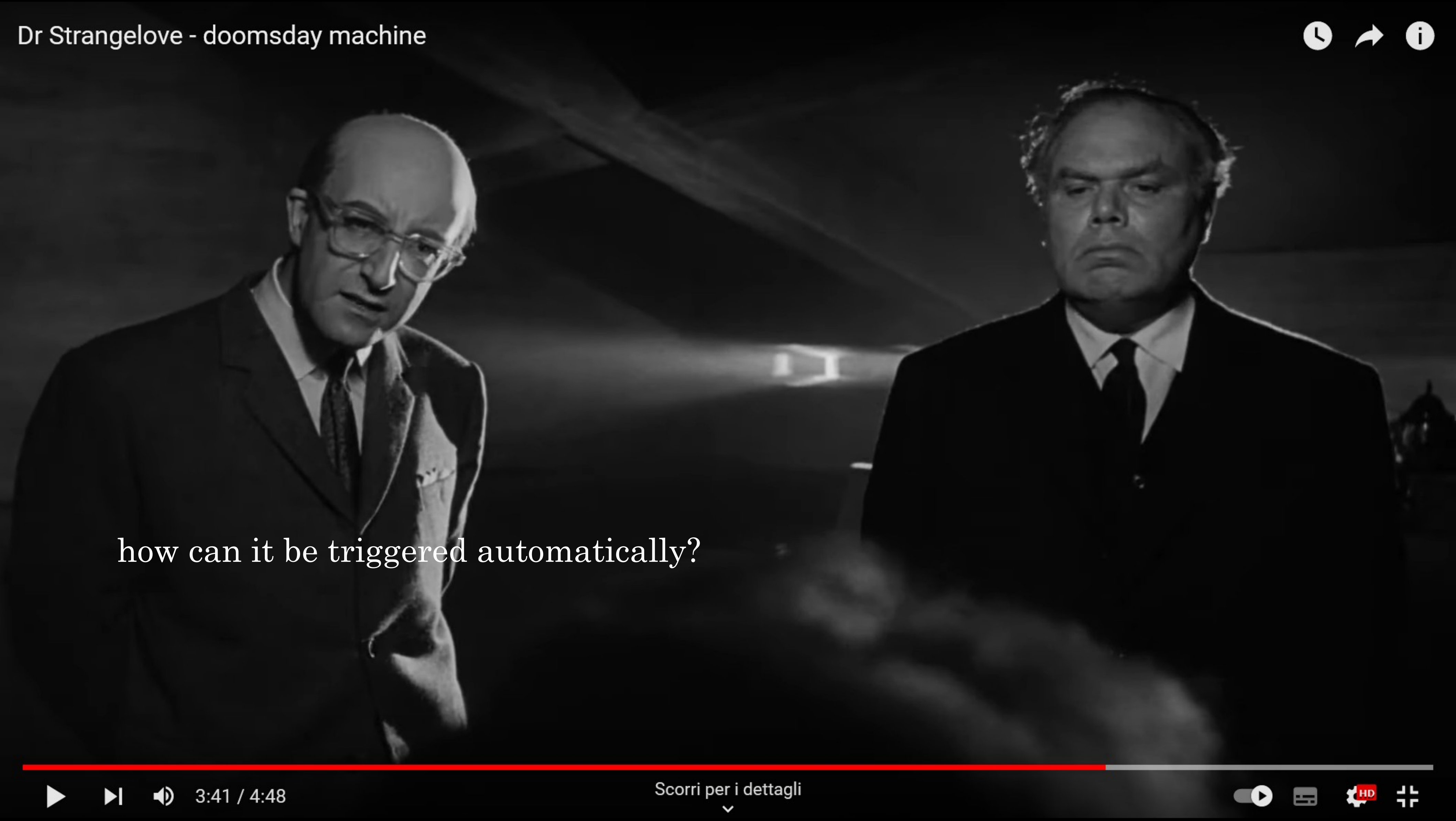
1964: Dr.Strangelove



Dr Strangelove - doomsday machine

the doomsday machine is designed to trigger itself automatically

1964: Dr.Strangelove



how can it be triggered automatically?

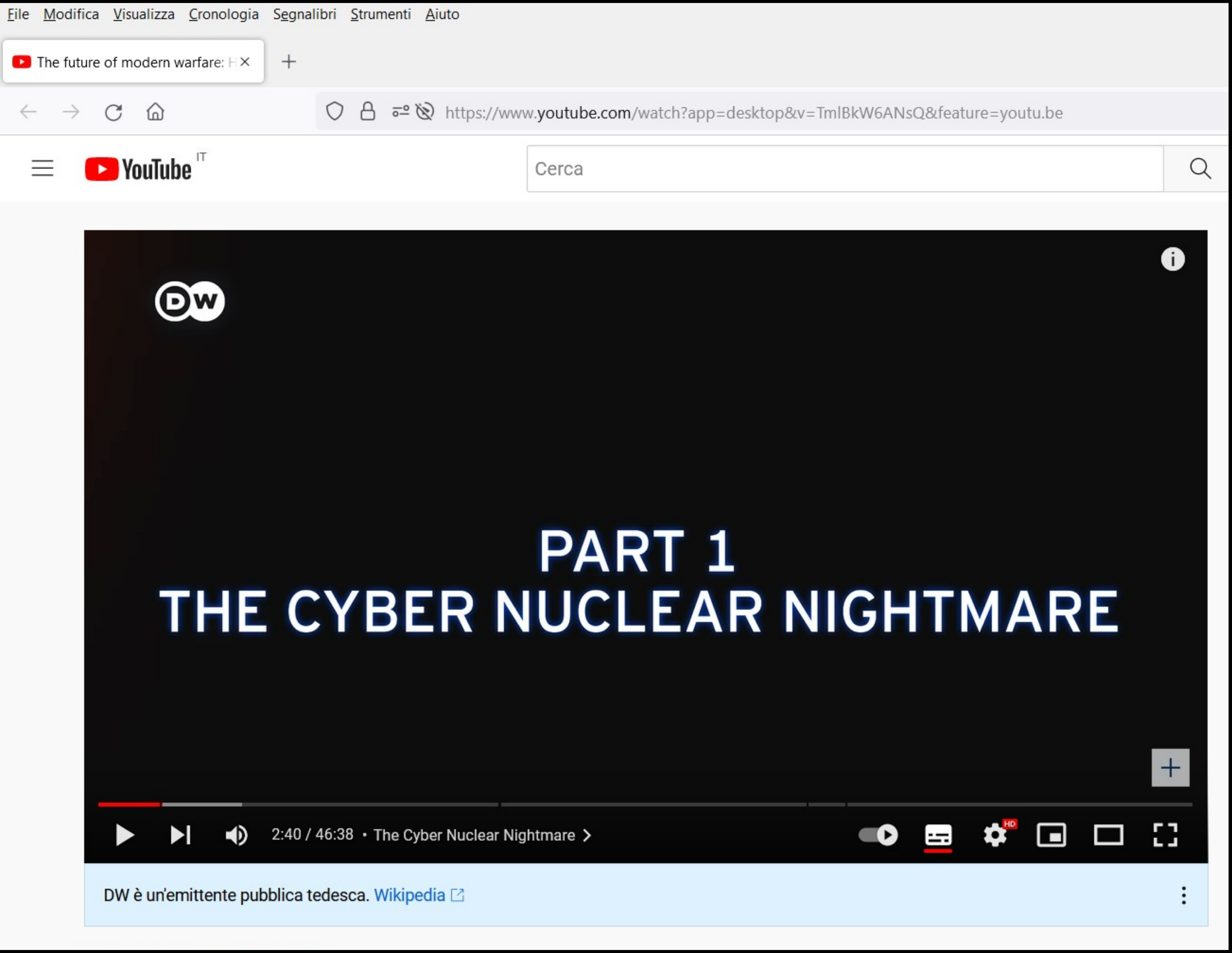
1964: Dr.Strangelove

…they are connected to a gigantic complex of computers

Grazie!

Insicurezze e responsabilità
nell'intersezione tra 'cyber and nuclear risk'

what if you find a malware in your early warning systems?


File
Modifica
Visualizza
Cronologia
Segnalibri
Strumenti
Aiuto
The future of modern warfare: H
https://www.youtube.com/watch?app=desktop&v=TmlBkW6ANsQ&feature=youtu.be
YouTube IT
Cerca
DW
2:40 / 46:38 • The Cyber Nuclear Nightmare

PART 1
THE CYBER NUCLEAR NIGHTMARE

DW è un'emittente pubblica tedesca. Wikipedia

https://www.youtube.com/watch?app=desktop&v=TmlBkW6ANsQ&feature=youtu.be