Advanced Sciences and Technologies for Security Applications

Gitanjali Adlakha-Hutcheon
Anthony Masys *Editors*

# Disruption, Ideation and Innovation for Defence and Security

Springer

# Advanced Sciences and Technologies for Security Applications

Indexed by SCOPUS

The series Advanced Sciences and Technologies for Security Applications comprises interdisciplinary research covering the theory, foundations and domain-specific topics pertaining to security. Publications within the series are peer-reviewed monographs and edited works in the areas of:

- biological and chemical threat recognition and detection (e.g., biosensors, aerosols, forensics)
- crisis and disaster management
- terrorism
- cyber security and secure information systems (e.g., encryption, optical and photonic systems)
- traditional and non-traditional security
- energy, food and resource security
- economic security and securitization (including associated infrastructures)
- transnational crime
- human security and health security
- social, political and psychological aspects of security
- recognition and identification (e.g., optical imaging, biometrics, authentication and verification)
- smart surveillance systems
- applications of theoretical frameworks and methodologies (e.g., grounded theory, complexity, network sciences, modelling and simulation)

Together, the high-quality contributions to this series provide a cross-disciplinary overview of forefront research endeavours aiming to make the world a safer place.

The editors encourage prospective authors to correspond with them in advance of submitting a manuscript. Submission of manuscripts should be made to the Editor-in-Chief or one of the Editors.

Gitanjali Adlakha-Hutcheon · Anthony Masys
Editors

# Disruption, Ideation and Innovation for Defence and Security

Springer

*Editors*
Gitanjali Adlakha-Hutcheon
Centre for Security Science
Defence Research and Development
Canada
Ottawa, ON, Canada

Anthony Masys
College of Public Health
University of South Florida
Tampa, FL, USA

ISSN 1613-5113 ISSN 2363-9466 (electronic)
Advanced Sciences and Technologies for Security Applications
ISBN 978-3-031-06635-1 ISBN 978-3-031-06636-8 (eBook)
https://doi.org/10.1007/978-3-031-06636-8

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Contents

Disruption

Ideation

## Innovation

## Back to Disruption

# Understanding the Landscape of Disruption, Ideation and Innovation for Defence and Security

**Gitanjali Adlakha-Hutcheon and Anthony J. Masys**

**Abstract** What do disruption, ideation and innovation have in common? How do disruptions, ideas and innovation coexist within defence and security? They all influence and impact decision-making. Disruptions drive decision-making. Ideation raises solutions to resolve the disruptions and innovation brings ideas into life. While disruptions may be common place in the business world, where disruptive technologies displace pre-existing ones; we are becoming more aware and sensitive to disruptions in the defence and security landscape stemming from new technologies and large-scale shocks on society such as the COVID-19 pandemic and climate change. For example, Saha and Chakrabarti (South Asian Surv 28:111–132, 2021: 112) argues that "COVID-19 has firmly established itself as the single largest security disrupter of this century in the non-traditional sense. It has necessitated a recalibration of securitisation framework…". Security disruptors that create challenges to global and national security interests manifest in events like "…the WannaCry cyber-attack, global terrorism, serious and organized crime, disease vectors, and natural disasters" (Masys in Handbook of security science. Springer, 2021). Such events are shaping the security calculus across health security, economic security, food security and energy security which are emerging as interrelated concepts that characterize the security landscape as complex. Weick and Sutcliffe argue that: "unexpected events often audit our resilience, everything that was left unprepared becomes a complex problem, and every weakness comes rushing to the forefront". (in 2007:2). With a defence and security landscape inundated with event and technological disruptions, the requirement for ideation and innovation becomes paramount. This edited book explores types of disruptions in defence and security, ways to assess disruptions triggered by technological advancements or the lack of legal frameworks; the consequent delays or disruptions to making decisions, creative idea generation and finally the innovative ways to counter such disruptions.

G. Adlakha-Hutcheon (✉)
Defence Research and Development Canada (DRDC), Ottawa, Canada
e-mail: gitanjali.adlakhahutcheon@gmail.com

A. J. Masys
International Centre for Policing and Security, University of South Wales, Newport, UK

G. Adlakha-Hutcheon and A. Masys (eds.), *Disruption, Ideation and Innovation for Defence and Security*, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-031-06636-8_1

**Keywords** Disruption · Ideation · Innovation · Shocks · Foresight · Security · Health security · Policing · Disruptive technologies

# 1 Introduction

Masys [1] describes how events such as '…the WannaCry cyber-attack, global terrorism, serious and organized crime, disease vectors, and natural disasters create challenges that affect both global and national security interests'. These transnational/transborder security challenges represent not only a threat to safety and security but also represent a disruption to our traditional views of national security characterized by state-based, military dimensions. Similarly, disruptive technologies such as AI, Quantum Computing, hypersonic weapons represent direct threats to national and global security. As described in Masys [2, 3], the threats and risks to human security (both man-made and natural) are varied and impactful. The distinction between natural and man-made threats is being blurred and the inherent vulnerabilities transcend this perceived dichotomy. Shocks (whether man-made or natural disasters) stress-test our 'human security' ecosystem often resulting in failures at various scales thereby posing serious threats nationally, regionally and globally. Given the complexity of the risk landscape as experienced through the COVID-19 pandemic nationally and globally [1], our mental models have been disrupted and require a fundamental redesign. To enable such a paradigm shift in how we view societal systems and address disruptions of security, ideation and innovation come into play.

# 2 Global National Security Disruptions

The World Economic Forum (WEF) 2021 Risk report highlights the major societal risks:

> …the highest likelihood risks of the next ten years are extreme weather, climate action failure and human-led environmental damage; as well as digital power concentration, digital inequality and cybersecurity failure. Among the highest impact risks of the next decade, infectious diseases are in the top spot, followed by climate action failure and other environmental risks; as well as weapons of mass destruction, livelihood crises, debt crises and IT infrastructure breakdown [4: 7].

These risks are shaping the security calculus across dimensions such as health security, economic security, food security and energy security emerging as interrelated concepts that characterize the security landscape as complex. Weick and Sutcliffe [5: 2] argue that: 'unexpected events often audit our resilience, everything that was left unprepared becomes a complex problem, and every weakness comes rushing to the forefront'. With a security landscape inundated with event and technological disruptions, the requirement for ideation and innovation becomes paramount.

These risks stemming from both man-made and natural disasters can be construed as disruptions to our societal and national security postures. Take for example the COVID-19 pandemic. As described in Masys [1]:

> COVID-19 is not a black swan. For years stemming from our experience with SARS, H1N1 and Ebola, Public Health and foresight experts have been calling attention to the global and national security impacts of global outbreaks. COVID-19 has in fact stress tested our national and global societal systems revealing inherent vulnerabilities within our societal systems and infrastructure in addition to vulnerabilities and shortcomings associated with our mindset.

From a security perspective, Agachi [6] describes the COVID-19 as:

> The novel coronavirus is… a canary in the coal mine. The pandemic is the harbinger of a security landscape marked by the rise of non-traditional security threats. These challenges will act as threat multipliers, further exacerbating existing security dilemmas…. COVID-19 is the template for what lies ahead, that is, unless we take action. The sooner we understand the fundamental transformation ahead of us, the sooner we can adapt our concepts and institutions to guarantee the safety of people, states, and the international community.

Likewise, the climate change discourse is changing the security calculus forcing a reflection on how we view national security and the global interdependence of threats and risk. The discourse regarding the disruptive implications of climate change on peace and security is manifest. A changing climate poses serious security risks and threats, both induced and amplified. Climate events disrupt national security that are revealed through regional and global instability. As described in Yassin and Cretti [7]:

> …in many parts of the world climate-related pressures, such as extreme weather events, rising sea levels or water scarcity threaten livelihoods and increase competition over food, water and land. If not appropriately addressed, the competition over such progressively scarce resources can turn into major security risks. Climate change can also trigger migration towards urban and less climate-stressed regions and increase socio-economic tensions among the population. When it is combined with other political or socio-economic pressures, its impacts can exacerbate existing drivers of insecurity and conflicts. Bearing this in mind, governments, international and local organizations across the world have realized the importance of designing context-specific practices to address security threats induced by climate change.

The International Military Council on Climate and Security (IMCCS) [8] argue that "It is therefore imperative that risks arising from climate change are systematically integrated into our security assessments as well as into our development, diplomacy, security and defense policies". One of the defining qualities of disruptive threats and risks as illustrated by COVID-19 pandemic and climate change is that '…national security is, in the borderless age of risks, no longer national security' [9]. As such, risk aetiology and in particular the security agenda has become complex and reflexive and it requires a reconceptualization of how we view security disruptions, ideation and innovation. As noted in Masys et al. [10: 773] 'The 'networked' understanding of hyper-risks [11] requires a more holistic approach to hazard identification and risk management, one that transcends the linear agent-consequence analysis and recognizes the transborder nature of disruptions.

## 3 Disruption, Ideation and Innovation

Unanticipated events can be a source of both disruption and opportunity. Whether through the introduction and application of novel technology or events that stress test societal systems, uncertainties, unintended consequences prevail. Risks and benefits are often not evenly distributed across populations thereby creating challenges to policymaking that support societal safety and security. Thus the question that arises is what is disruption? The Merriam-Webster Dictionary[1] defines disruption as "the act or process of disrupting something: a break or interruption in the normal course or continuation of some activity, process, etc. and includes derangement, dislocation, disturbance, and upset as its synonyms. The word itself was first used back in 1622. Are disruptions only negative? The term disruption and its synonyms would have one believe so. What about the birth of a first child? A new born is certainly disruptive to the life of the parents yet a welcome interruption for most, suggesting that the effect or the consequence of a disturbance must also be examined in discussions about disruptions. And then disruptions could be large or small, where the latter too can set off ripples which in of themselves are big disruptors. The Covid-19 pandemic represents such a disruption to global health security, economic security and human security. As highlighted in Masys [1] "For years stemming from our experience with SARS, H1N1 and Ebola, Public Health and foresight experts have been calling attention to the global and national security impacts of global outbreaks. COVID-19 has in fact stress tested our national and global societal systems revealing inherent vulnerabilities within our societal systems and infrastructure in addition to vulnerabilities and shortcomings associated with our mindset". The International Risk Governance Center (IRGC) [12] states that "external shocks to interconnected systems, or unsustainable stresses, may cause uncontrolled feedback and cascading effects, extreme events, and unwanted side effects, implying that the potential for cascading disruption is a growing and critical concern for many facets of daily life". Disruptions can be differentiated on the basis of their causative triggers, for example ones triggered by technology, or by law or its lack thereof.

An example of a disruption of the twentieth century, bar none, is programmable computers, therefore not a disruption but ***the*** disruption. The disruption of the twentieth century is programmable computers with no close second. Is there one already known within the twenty-first century? At what scale. Yes, the COVID-19 pandemic was/is a disruption but the world is managing. The ongoing pandemic is disruptive but it could have been worse, therefore one is back to asking what is a disruption? It is a term used time and again and all too often in a general sense. Therefore the intuitive follow-on questions become: Is there a metric for it? A measure of disruptive potential? What do the editors and authors count as Disruption? On the one hand disruption is occurring at the scale of Climate change, on another it is the pandemic. Both climate change and the pandemic are large, are expressed at societal levels and fraught with inherent complexity. An interpretation is that these examples

[1] "Disruption." Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/disruption Accessed 21 Dec. 2021.

are counted as disruptions at close to immeasurable levels. Following this train of thought, a disruption is one that cannot be countered, and therefore demands problem solving, critical thinking, ideation and more. Of course, ideation and or innovation are only relevant if the disruption is of the type that can be addressed—technology-triggered or triggered by delayed decisions. It is the latter type that will largely be the subject of this book.

In an introduction it is also important to note what Disruption is not…It is not a safe bet, not fast and not necessarily obvious…according to Peter Daisyme.[2] He gives examples of disruptions Google, Uber and Tesla as non-disruptors and calls Tesla an innovation. The editors suggest that all three are examples that call into question a business system around technological advancement.

What then are the types of Disruptions related to Defence and Security? The introduction of novel prototype weapon systems such as military hypersonic weapons is being framed as a 'Sputnik' moment that can shift regional and global balances of power. Similarly, the advent of artificial intelligence in support of defence operations is viewed as a game changer for intelligence applications, security applications and operational employment of weapon systems. Within the defence sphere, in particular with the 'war on terror', we have witnessed the dual nature of technology applications. For example, as detailed in Liang [13], '…terrorists have proved to adapt over the past two decades, they have been able to innovate not only in their organizational structure, becoming decentralized, franchised and technologically savvy, but they have also evolved in the operational and tactical sphere in their military operations. Their tactics have also evolved from irregular guerrilla warfare to indiscriminate attacks to a greater sophistication in harnessing new and emerging technologies… Since 2016, ISIS has been using drones to carry out intelligence, surveillance, and reconnaissance missions. ISIS also conducted attacks with drones carrying explosives which were used to kill enemy combatants in northern Iraq'.

How should disruptions be measured or assessed? Is the mechanism of assessment of disruption the same for that which is caused by Emerging and Disruptive Technologies[3] or differs from that caused by Law, even as both call for professional judgement and/or interpretation? If one accepts that the nature of disruptive innovations is multidimensional as originally proposed by Cristensen,[4] then one has on hand a framework to assess potential disruptiveness of product innovations developed by Guo et al.[5] as well as a game-based, future-oriented table-top exercise called Methodology for Assessing Disruptions or MAD [14] that assess the delta in the course of action taken by opposing teams as a measure of the disruption that can be caused by creative ideas for innovations [14]. The MAD games have successfully been used in defence research [15] as well as by industries toward determining where next to invest. Tools to assess disruptions [16] provide insights necessary for devising ways to address disruptions, occurring on a variety of scales and punctuated or ongoing

[2] What Is Disruption, Really? 8 Examples and What to Learn From Them|Startup Grind

[3] 210303-EDT-adv-grp-annual-report-2020.pdf (nato.int).

[4] Disruptive Technologies: Catching the Wave (hbr.org).

[5] https://doi.org/10.1016/j.techfore.2018.10.015.

in time. It is here that systematically being creative in the generation of ideas or ideation, and being innovative to forge the way ahead, come in.

This book is arranged in three sections, one each on Disruption; Ideation; and Innovation. It is acknowledged that each chapter within each section does not stay cleanly within the bounds of one of these umbrella terms, and nor should they given the nature of their overlap.

**The Section on Disruption** has three chapters.

The book leads off with a chapter on the centrality of human in a system. It speaks to the agency that a human provides in not only evading disruption but also enhancing the reliability of a system using the Cold War as an example; it is titled: *System reliability: a Cold War Lesson.* The following chapter addresses an anticipated technological disruption riding on the waves of quantum computing power in the realms of defence and security; it is titled: *Quantum computing: unraveling the hype.* The next chapter continues the examination of the disruptiveness of technologies and does so from the standpoint of a greater understanding of the unexpected as a way to become aware of their innovative potential; it is titled *Emerging and disruptive technologies and security: Considering trade-offs between new opportunities and emerging risks.* Lastly, while not in this, the first section, the final chapter in the book touches upon disruption at the grandest of scales, that is to say at the level of society with fifth generation warfare, a new form of warfare that spans across technology, human and hype. It is titled: *Fifth Generation Warfare? Violent transnational movements as security disruptions.*

## 4 Section 2: Ideation

Ideation is a noun, the capacity for or the act of forming or entertaining ideas, first used in 1818 according to the Merriam-Webster Dictionary.[6] The synonyms for ideation include what one would imagine, these range from creativity, fancy, fantasy, imagination, imaginativeness, invention, inventiveness, and originality to even contrivance.

Ideation is used for developing new products, and is founded on design thinking. The generation of ideas being critical in engineering design processes, has spurred an entire discipline, variously named Design thinking, Engineering Design, etc. within graduate schools for Architecture and Business. As a result research efforts have focused on developing idea generation tools to aid designers in exploring design possibilities. There is even research to evaluate metrics for design exploration, even

[6] "Ideation." Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/disruption. Accessed 21 Dec. 2021.

one[7] proposing a single metric to compare idea generation processes and methodologies. Tools of ideation range from the use of board games[8] to use of techniques like brain writing. It is worth noting that by and large, tools used for ideation spark creativity and tend to stop there. Going the extra mile is what extends ideation into innovation.

In adapting from the business world, the use of processes for ideation as applicable to the world of defence and security is what is of interest here. Can ideation aid disruption? Advance or cause more disruption? Since the delineation from disruption to ideation or for that matter between ideation and innovation is not a clean crisp line, so too each chapter does not only speak to one of these terms.

The **section on Ideation** is comprised of three chapters. The first that explores human systems as a means to systematically address all disruption, ideation and innovation in defense and security systems and posits that human system exploration or HSE is "especially relevant with regard to defense and security technology as their (its) application can affect human lives and integrity". It is titled: *Human Systems Exploration for Ideation and Innovation in potentially disruptive Defense and Security Systems.* The next chapter lays the groundwork for innovation. It is titled: *Total War: a context for cybersecurity innovation.* The last chapter within the Ideation section is titled: *The Impact of the Internet and Cyberspace on the Rise in Terrorist Attacks across the US and Europe.* In it the authors analyze the relationship between a so-called disruptive technology, the internet, and its ability to lead to terrorist attacks only to arrive at the conclusion that it is not easy to relate the cause and effect. Thus, in turn invoking the question whether the internet really has a continual disruptive effect with respect to terrorism? More importantly, and more germane to the theme of Ideation, whether analyses constitute a form of generation of ideas?

Among the trio of disruption, ideation and innovation, ideation is the most modern of words in terms of usage, thereby also providing evidence for the evolution of language.

## 5 Section 3: Innovation

The earliest use of innovation,[9] an adjective, is in the 15th C to reflect a new idea, method, or device: a NOVELTY, the introduction of something new. The synonyms of innovation include brainchild, coinage, concoction, contrivance, creation and invention. Yet, the dictionary makes a distinction between invention and innovation. Invention can refer to a type of musical composition, a falsehood, a discovery, or any product of the imagination. The sense of invention most likely to be confused

[7] https://doi.org/10.1016/j.destud.2009.07.002.

[8] Our favorite ideation tools—Board of Innovation, https://www.boardofinnovation.com/staff_picks/our-favorite-ideation-tools/.

[9] "Innovation." Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/disruption. Accessed 21 Dec. 2021.

with innovation is "a device, contrivance, or process originated after study and experiment," usually something which has not previously been in existence.

Innovation, for its part, can refer to something new or to a change made to an existing product, idea, or field. One might say that the first telephone was an invention, the first cellular telephone either an invention or an innovation, and the first smartphone an innovation. Thus for an innovation to exist, first an idea has to come in to being, and then, invented in to an innovation.

Five chapters constitute the **section on Innovation** which explores the question of how can innovative ideas address disruptions. For instance can even emerging disruptive technologies such as cognitive aids assist with decision-making and thus prevent disruption? The section begins with the types of innovations required to counter shocks and disruptions in defence and security; it is titled *Shocks and Disruptions in Defence and Security: How to lead by Inspiring Innovation through Ideation*? The next chapter speaks to an innovative technology-centric networked platform integrated with policies to not only counter the disruption caused by malaria in Uganda but also to provide much-needed health security, it is titled: *Health security and malaria: a neural network iOS intelligent platform for implementing Seek and Destroy Integrated Vector Management (IVM) policies.* The following chapter connects biological and technological systems in a discussion of Convergence, as is also its title: *Convergence.* The chapters that follow are about innovations in policing through the use of legal principles toward disruptive technologies or anticipatory intelligence. These are titled: *Legal principles governing disruptive technologies in policing: legal innovations?*, and *Being two steps ahead: the added value of anticipatory intelligence analysis in law enforcement*, respectively.

This book offers researchers and scholars alike a glimpse into different types of disruptions, grounds to counter disruptions through ideation and innovation, thereby bolstering defences and enhancing security *writ large.* Its ultimate hope is to incite an innovation warfare that minimizes disruptions from occurring in the first place, but then, is this even possible?

## References

1. Masys AJ (2021) Non-traditional Security: a risk centric view. In Masys AJ (ed) Handbook of security science. Springer
2. Masys AJ (ed) (2016) Disaster forensics: understanding root cause and complex causality. Springer
3. Masys AJ (ed) (2016) Exploring the security landscape- non-traditional security challenges. Springer
4. WEF (2021) The global risks report 2021. https://www.weforum.org/reports/the-global-risks-report-2021
5. Weick KE, Sutcliffe KM (2007) Managing the unexpected: resilient performance in an age of uncertainty, 2nd edn. Wiley, San Francisco, CA
6. Agachi A (2020) The Miner's Canary: COVID-19 and the rise of non-traditional security threats. https://www.defenseone.com/ideas/2020/05/miners-canary-covid-19-and-rise-non-traditional-security-threats/165446/

7. Yassin M, Cretti G (2021) Turning climate-security into meaningful practices to promote peace. https://www.planetarysecurityinitiative.org/news/turning-climate-security-meaningful-practices-promote-peace
8. IMCCS (2021) https://imccs.org/wp-content/uploads/2021/06/World-Climate-Security-Report-2021_Key-Risks-and-Opportunities.pdf
9. Beck U (2002) The terrorist threat: world risk society revisited. Theory Cult Soc 19(4):39–55
10. Masys AJ, Ray-Bennett N, Shiroshita H, Jackson P (2014) High impact/low frequency extreme events: enabling reflection and resilience in a hyper-connected world. In: 4th international conference on building resilience, 8–11 September 2014, Salford Quays, United Kingdom. Procedia Economics and Finance 18(2014):772–779
11. Helbing D (2013) Globally networked risks and how to respond. Nature 497:51–59
12. IRGC (2018) Guidelines for the governance of systemic risks. International Risk Governance Center (IRGC), Lausanne
13. Liang C (2022, in press) Far-right contagion: the global challenge of transnational extremist networks. In Masys AJ (ed) Handbook of security science. Springer
14. Adlakha-Hutcheon, G, Hazen M, Hubbard P, Mclelland S, Sprague K, (2012) Methodology for Assessing Disruptions (MAD) Part I—report and analysis, Defence Research and Development Canada, Technical Memorandum 2012–009, Methodology for Assessing Disruptions (MAD) Game Part I: Report and Analysis (dtic.mil)
15. Adlakha-Hutcheon G (2017) The MAD Way, Proceedings of the Tenth Annual NATO Operations Research & Analysis Conference, NATO Science & Technology Organization website, Defence and Research Development Canada, DRDC-RDDC-2016-P172, NATO MP-SAS-OCS-ORA-2016–11
16. Adlakha-Hutcheon G, Wallace B, Jovic S (2020) Exercising MADness—Countering Civil Unrest: Results of Workshops Conducted at the International North Atlantic Treaty Organization Concept Development and Experimentation Conference, Defence and Research Development Canada, Scientific Letter, DRDC-RDDC-2020-L289
17. Saha S, Chakrabarti S (2021) The non-traditional security threat of COVID-19 in South Asia: an analysis of the Indian and Chinese leverage in health diplomacy. South Asian Surv 28(1):111–132

# Disruption

# System Reliability: A Cold War Lesson

**Simon Bennett**

**Abstract** Defence technologies, such as early-warning systems, are subject to exogenous and endogenous threats. The former may issue from jamming or, in a combat situation, anti-radiation missiles. The latter may issue from latent errors (Reason in Human Error. Cambridge University Press, Cambridge, 1990) introduced into the system at the initial design stage or during an upgrade, that is, through reactive patching (Weir in Debates in Risk Management. UCL Press, London, pp 114–126, 1996). It is easier to defend against exogenous than endogenous threats. Nevertheless, mindfulness when designing or upgrading a defence system reduces the risk of latent or embedded errors compromising reliability. This chapter will argue that systems that permit manual intervention, that is, manual override, are more reliable than systems that provide little or no opportunity for intervention. Referencing a Cold War near-miss, the chapter posits a negative relationship between coupling and reliability. That is, the more tightly coupled—that is, automated and linear—a system's architecture, the less reliable it will be (other things remaining equal). It has become fashionable to characterise the human component as a liability—a latent error. The manner in which the Cold War crisis described below was resolved demonstrates the unfairness, indeed, recklessness of this characterisation.

**Keywords** Defence · Socio-technical systems · Coupling · Reliability · Human component · Asset

## 1 Introduction

Those who stand to make a great deal of money out of automation are peddling a myth—that automated systems are reliable and invariably more dependable than systems that require operator input [3]. Unfortunately for the fortune-seekers, the reality is that technology is—and probably always will be—fallible. It is fallible:

S. Bennett (✉)
Civil Safety and Security Unit, University of Leicester, Leicester, England
e-mail: sab22@leicester.ac.uk

G. Adlakha-Hutcheon and A. Masys (eds.), *Disruption, Ideation and Innovation for Defence and Security*, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-031-06636-8_2

- because it is designed in the context of imperfect knowledge about future conditions
- because system phenomena such as interactive complexity, non-linear interactions and emergence [18], and organisational phenomena such as reactive patching [32], negatively impact reliability and performance.

These claims can be corroborated. Arlindo Oliveira [22, 487] of Lisbon's Instituto Técnico observes: "In engineering there is no such thing as 100% reliability or 100% precision. Every system that is designed to perform a specific task will have a probability of failure, however small …". Peter Herena [16] of the American Institute of Chemical Engineers observes: "While designing something that never fails is a lofty and admirable goal, it's not wholly realistic …". Aviation safety advocate Charles Billings [4, 5–6] observes: "Several [aviation] accidents, and a larger number of incidents have been associated with, and in some cases may have been caused by, aircraft automation …. In some cases, automated configuration warning devices have failed …. In other cases, automation has operated in accordance with its design specifications, but in a mode incompatible with safe flight under particular circumstances. In still others, automation has not warned … that the automation was operating at its limits, or was operating unreliably …. It is … clear that certain costs have been associated with automation …". Whatever automation's advocates may claim, technology is not infallible.

Technology's fallibility is evident in road transportation. Consider the Uber self-driving car accidents. In 2017, Uber took its self-driving vehicles off the road following an accident in Arizona. In 2018, a pedestrian was killed in Tempe, Arizona, by an Uber self-driving vehicle. At the time of the accident the vehicle was in autonomous mode with a human monitor behind the wheel.

There have been other accidents involving similar technologies. In May, 2016, a Tesla Model S collided with a lorry while in semi-autonomous Autopilot mode. The Tesla driver was killed. According to the National Transportation Safety Board, Tesla's Autopilot system was partly to blame for the fatal accident. On 23 March, 2018, a Tesla Model X automobile crashed into a highway barrier while in semi-autonomous Autopilot mode. The car caught fire. The driver died. At the time of the collision, the driver's hands were not on the steering wheel. In March, 2019, a Tesla Model III driver died when his vehicle hit a truck while in Autopilot mode: "The roof of the car was sheared off …. [T]he driver did not appear to have his hands on the wheel, and neither he, nor the Autopilot, took any evasive action" [6]. A former US Secretary of Transportation referred to the 2018 Tempe, Arizona, fatal accident as " … a wake-up call to the entire [autonomous vehicle] industry and government to put a high priority on safety" (Foxx cited in [5]). Lobby group Consumer Watchdog said: "We hope our calls for real regulation of driverless cars will be taken seriously by Silicon Valley …" (Consumer Watchdog cited in [5]).

Technology's fallibility is evident in aviation. Consider the 2018 and 2019 Boeing 737MAX-8 accidents. In each accident, the aircraft's Manoeuvring Characteristics Augmentation System (MCAS), an automated system designed to compensate for the re-engined aircraft's tendency to pitch-up under certain operating conditions, repeatedly pushed the nose down until the aircraft hit the ground. The MCAS's reliance on inputs from a single angle-of-attack sensor meant it was vulnerable to sensor miscalibration or malfunction [30]. Further, the MCAS's capacity for rapid serial activation risked pilots becoming task-saturated. Overburdened pilots underperform: "[O]nce the level of arousal becomes high, performance starts to deteriorate and people make errors" [15, 70]. Three hundred and forty-six passengers and crew died in the accidents. The MCAS—an automated system—transformed a previously reliable and successful aircraft into an unreliable aircraft that trashed Boeing's reputation and balance-sheet.

Technology's fallibility is evident in astronautics. Consider the curtailment of the December, 2019, Boeing Crew Space Transportation-100 (CST-100) Starliner Orbital Flight Test 1 (OFT1). On 20 December 2019, an unmanned Boeing Starliner capsule was subjected to a rigorous proof-of-concept test (Fig. 1). The test, which would have seen the Starliner capsule dock with the International Space Station (ISS), went badly: "The spacecraft's on-board computer was off by 11 hours—a significant software problem that went undiscovered because Boeing's preflight testing was cut short and used a faulty computer simulator. While Starliner was in flight, Boeing uncovered another software problem that should have been unearthed by testing on the ground—one that could have caused the service module to crash into the crew module before the spacecraft was re-entering the atmosphere" [9]. The two software bugs, together with a telemetry issue, persuaded the NASA to curtail the mission. There was no docking. The NASA claimed it had curtailed OFT1 because Starliner did not have enough fuel to reach the ISS. A cynic might argue that OFT1 was curtailed not because the Starliner lacked the fuel to reach the ISS, but because the NASA, having lost confidence in Boeing's software and telemetry, feared the Starliner might collide with its iconic and irreplaceable ISS.

Technology's fallibility is evident in defence. On 3 June, 1980, at 02:26, a US General telephoned the President's National Security Adviser to inform him that the Soviets had launched 220 intercontinental ballistic missiles (ICBMs) against the United States. In a second telephone call, he informed the National Security Adviser that, in fact, the Soviets had launched 2,200 ICBMs against the US. With the National Security Adviser about to inform the President, the general telephoned him a third time. He explained that there was no attack and that the alert had been triggered by a single, faulty computer processor buried deep inside a communications system at the headquarters of the North American Air Defence Command (NORAD) [19]. During the alert, the US had prepared for war: "U.S. Air Force ballistic-missile crews removed their launch keys from the safes, bomber crews ran to their planes, fighter planes took off to search the skies, and the Federal Aviation Administration prepared to order every airborne commercial airliner to land" [28]. Given tensions between the US and USSR over Afghanistan, a Soviet decapitation strike was far from implausible: "The Soviets had recently invaded Afghanistan, and the animosity between the two superpowers was greater than at any other time since the Cuban Missile Crisis" [28]. The day was saved by the defence-in-depth of America's ICBM early warning-system—its radars had not seen any ICBMs arcing above the horizon—and by the fact that a nuclear assault on the Soviet Union could not be launched without the President's authorisation. Thankfully for humankind, the machinery of war was not managed entirely by computer algorithms. Interestingly, the 1980 NORAD microprocessor-induced near-miss was presaged in the 1962 novel *Fail-Safe*, written by political scientists Eugene Burdick and Harvey Wheeler. In Burdick and Wheeler's [7] seminal work, an attack by the US on the USSR is triggered by a computer malfunction. The 1964 film of the book, produced by Columbia Pictures and directed by Sidney Lumet (who later directed Serpico), is thought-provoking.

Designers use a variety of strategies to imbue systems with resilience. For example:

- redundancy, wherein key components or sub-systems are duplicated or triplicated. Redundancy may be referred to as defence-in-depth or the belt-and-braces approach to safety
- failsafe mechanisms that enable a component or sub-system to fail without jeopardising the host system and/or its surrounding environment. A failsafe mechanism is one that, in the event of a component or sub-system failure, " … will not leave the [system in question] outside its operating limits" [4, 148]. A system that fails-safe " … is designed in [such] a way … that when a failure does occur, the device will tend to fail in a predictable manner to a 'safe state'" [16]

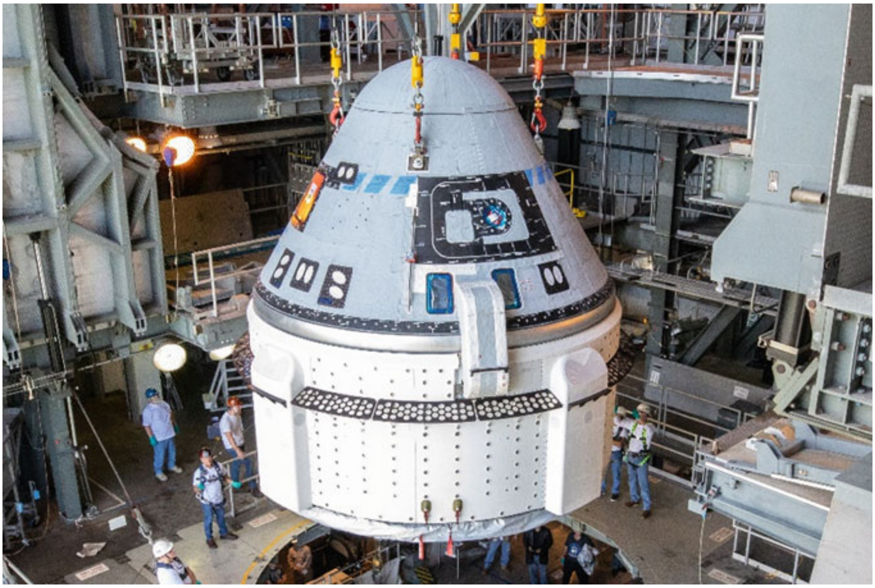

**Fig. 1** A Boeing-manufactured Starliner capsule being mated with an Atlas 5 rocket. Software bugs and a telemetry issue forced the curtailment of the December, 2019, OFT1 shakedown test. Technology is fallible (Wikimedia [36])

- loose coupling, wherein operators are provided opportunities to assume manual control of an errant system. Only if operators are provided adequate amounts of timely, high-quality data on the status and performance of the system can they hope to successfully assume manual control: “If the human operator is not involved in on-line control, he will not have detailed knowledge of the current state of the system. One can ask what limitations this places on the possibility for effective manual take-over, whether for stabilisation or shut-down of the process, or for fault diagnosis” [2, 777]. Billings [4, 148] observes: “Automation of unavoidably complex procedures … is necessary and entirely appropriate, provided the human is kept apprised so he or she understands what is going on. The system must be able to be operated by the human if the automation fails”. Professor Charles Perrow, the man behind normal accident theory [23], would argue it is not a matter of ‘if’, but when, and under what circumstances, the automation fails. In 1983, at a time when relations between the USSR and US were under great strain [10], a Soviet early warning satellite mistook a natural phenomenon for multiple intercontinental ballistic missile (ICBM) launches, precipitating an alarm that could have seen much of the world destroyed in an all-out nuclear war.

## 2 The 1983 War Scare

### *2.1 Geopolitical Context*

Following the 1962 Cuban Missile Crisis that left the world teetering on the edge of nuclear Armageddon, the US and USSR strove to reduce tensions. Thanks to détente, the 1970s saw no nuclear near-misses between the superpowers, although, *gratis* numerous proxy wars, such as that between North and South Vietnam, tensions remained high. Neither the USA nor the USSR was willing to cede ground to the other. Each invested heavily in new weapons systems, the Carter administration, for example, investing in the Pershing II intermediate-range nuclear missile, the Gryfon ground-launched cruise-missile (GLCM) and the multi-warhead MX missile [8]. The Pershing II’s accuracy and short launch-to-impact time made a nuclear decapitation strike against the USSR a practical option: “In 1983, the Americans began deployments in Western Europe of the Pershing II … which had a flight-time to Moscow from West Germany of 4–6 minutes in what was termed ‘a super-sudden first strike’ capability” [10, 2].

Détente, on its death bed during the Carter administration, met its end during the Reagan administration (Fig. 2). President Reagan’s bullishness saw relations between the two superpowers deteriorate to the point where the Soviet leader, the ailing Yuri Andropov, former head of the KGB, convinced himself that Reagan might be tempted to launch a nuclear decapitation strike against the USSR [10]. On March 23, 1983, Reagan announced his Strategic Defence Initiative (SDI) that would, at least on paper, have made the USA invulnerable to nuclear attack. Reagan’s announcement convinced Andropov that his view of the President as a warmonger was correct.

**Fig. 2** The US President with the British Prime Minister. Reagan theatrically dubbed the USSR the Evil Empire, a soubriquet that greatly irritated the Soviets [10, 34]

Fischer [12, 17] writes: "Four days after the President's announcement … Andropov lashed out. He accused the United States of preparing a first-strike attack on the Soviet Union …. Andropov's remarks were unprecedented …. For the first time since 1953, the top Soviet leader was telling his nation that the world was on the verge of a nuclear holocaust". The stage was set for a confrontation.

## 2.2 *Doctrinal Context*

With the development in the 1950s of the intercontinental ballistic missile (the Soviets test-launched the first ICBM, the R-7, in 1957), a doctrine was required to effectively manage the threat posed by missiles with a launch-to-impact time of *circa* 35 minutes [11]. Faced with the prospect of express annihilation, the Soviets settled on a policy of launching their ICBMs the moment they suspected they were under attack. If actioned, the Soviets' Launch on Warning policy would have seen its missiles destroy much of the continental United States. Reviewing the Soviets' Launch on Warning posture, the Central Intelligence Agency (CIA) concluded it was doubtful the Soviets would wait until they were under attack before launching their missiles. The CIA believed it possible the Soviets would launch their missiles if they suspected the US was preparing to attack [8]. Thus, in the 1980s, each side believed the other capable of launching a pre-emptive strike. Andropov was as suspicious of the US as Reagan was of the USSR. It was against this background of mistrust and hair-trigger defence postures that the 1983 War Scare occurred.

The Soviets' Launch on Warning posture, intended to deter nuclear belligerence, had a number of consequences:

- it raised the prospect of mutual assured destruction (MAD)
- it required early-warning systems that could reliably identify missile launches against the Soviet Union
- it required a system of command-and-control that could reliably interpret data produced by early-warning systems well within the *circa* 35 minutes launch-to-impact window.

By 1983, the two superpowers possessed *circa* 18,400 nuclear warheads [11] (Fig. 3). A Soviet strike against the US would have inflicted massive damage: "[In the first 24-hours] Moscow would have been capable of delivering 4,000 nuclear warheads … onto the US … reducing the American population by half … and the country's industrial base by 70%" [10, 2].

## 2.3 The War Scare

On 26 September, 1983, during NATO's Autumn Forge military exercise, a Soviet spy satellite, Kosmos-1382, misinterpreted reflected sunlight for missile launches. The system of which Kosmos-1382 was a part then informed Lieutenant-Colonel Stanislav Petrov, safely accommodated in the Serpukhov-15 Early Warning Centre south of Moscow, that the United States had launched five missiles against the USSR. The missile launches were reported serially until, according to Petrov, the early-warning computer was "roaring" (Petrov cited in [17]). Petrov recalled what happened in an interview with the British Broadcasting Corporation (BBC): "The siren howled, but I just sat there for a few seconds, staring at the big, back-lit red screen with the word 'Launch' on it …. A minute later, the siren went off again. The second missile was launched. Then the third, and the fourth and the fifth. Computers changed their alerts from 'Launch' to 'Missile Strike' …. I couldn't move. I felt like I was sitting on a hot frying pan" (Petrov cited in [1]). Throughout the alert, there was no indication from the hardware or software that there had been a malfunction: "Petrov's computer systems said the reliability of the satellite's information was at the 'highest' level" [29].

Fortunately for the startled Petrov, the system was not so tightly coupled that it did not afford him time to reflect before he talked to senior commanders. As he observed: "There was no rule about how long we were allowed to think before we reported a strike" (Petrov cited in [29]). Although under pressure [11], Petrov correctly concluded that the satellite and its associated computer algorithms had generated false positives. That is, that the indications picked up by the satellite's infra-red sensors had been produced by something other than missile launches (it

**Fig. 3** A test launch of a US Minuteman III ICBM. In the 1980s, America's missile fields were populated with Minuteman II and Minuteman III ICBMs. Today's nuclear weapons are orders of magnitude more powerful than the crude devices dropped on Hiroshima and Nagasaki [33]

was discovered that they had been produced by sunlight reflected off high altitude clouds).

Petrov, in concluding it was a false alarm, was guided by reason and fact. He reasoned that a decapitation strike would see the US launch not five ICBMs, but all of them: "When people start a war, they don't start it with only five missiles. You can do little damage with just five missiles" (Petrov cited in [17]). He knew that Kosmos-1382's optical sensors had not registered any rocket plumes. He knew that none of the USSR's ground-based early-warning radars had detected ICBMs arcing above the horizon. Having evaluated the evidence rationally, Petrov concluded that the USSR was not under attack. The Lieutenant-Colonel resiled from recommending a retaliatory strike [11]. Petrov described his reasons for resiling in a March 2004 interview with a Danish newspaper: "I gave the Americans the benefit of the doubt …. By that time, the Americans had not yet developed a national missile defence system—they still haven't—so they knew that a nuclear attack on us was tantamount to the eradication of at least half of their population. I was convinced that the Americans were a militant nation, but not a suicidal one. I remember thinking, 'That big [of] an idiot has not been born yet, not even in the US'" (Petrov cited in [20]).

The episode is interesting sociologically. First, because the Soviets, when designing their satellite-based early-warning system, left room for human judgment. They could have introduced a fully automated, algorithm-based system. They chose not to, perhaps because, like Charles Perrow [23], they understood that technology is fallible, and because, like Professors Erik Hollnagel, Robert Wears and Jeffrey Braithwaite [18], they considered human operators assets rather than liabilities: "Humans are … a resource necessary for system flexibility and resilience" [18, 4]. Petrov's testimony suggests the Soviet Union's military leaders were right to be skeptical about the reliability of their satellite-based early-warning system. Petrov, a skilled analyst and programmer who had helped install the system [11], described it as "raw" (Petrov cited in [17]). Downing [11, 195] observes: "[Soviet] scientists were pushed by the political and military leaders to get Oko [the USSR's satellite-based early-warning system. Oko means 'eye'] into operation well before all the glitches and problems had been ironed out. They were told it was a matter of urgent national defence and no delay was allowed; problems could be rectified after the system had become operational". In her celebrated book *Hello World: How to be Human in the Age of the Machine*, mathematician Hannah Fry [14] questions the ability of computer algorithms to consistently produce reliable decisions, especially if their logic is suspect and their working data inadequate and/or unreliable. Fry, like the Soviet scientists who left room in the Oko system for human judgment, is wary of automation. The curtailment in December, 2019, of OFT1 suggests such skepticism to be appropriate.

The episode is interesting sociologically because it interposed someone willing and able to think and act independently into a rigid hierarchy populated by individuals who were expected to follow orders and adhere to procedure. Lieutenant-Colonel Stanislav Petrov, Deputy Chief of the Department of Military Algorithms, was out of step with his colleagues. Publicly educated, the donnish Petrov was never fully at ease with the Soviet military's authoritarian mindset. Reflecting on his situation, Petrov observed: "My colleagues were all professional soldiers, they were taught to give and obey orders …. [T]hey were lucky it was me on shift that night" (Petrov cited in [1]). Interestingly, Petrov was on duty on the night of the War Scare by accident—he was standing in for a sick colleague. An inductive analysis of Petrov's management of events on the night of 26 September, 1983, suggests that where designers provide human operators opportunities to verify whether or not a system is operating within limits, those operators must be willing and able to think independently and act decisively, whatever the consequences for the system, their colleagues, their organisation and themselves. Operators with decision-making power must have integrity.

Following the events of that night, Petrov fell victim to the fundamental attribution error (see Fiske and Taylor [13] for a definition). The military blamed him for the War Scare: "The following year [1984] [Petrov] was discharged from the Soviet military. Petrov felt … that he was being personally blamed for the failure of the satellite surveillance and computer systems. He found himself out of work with his pension massively cut back" [11, 200]. Following the War Scare, the authorities charged Petrov with not keeping a log of the events of 26 September. Petrov's defence was that during the emergency he had a telephone in one hand and a public address system in the other. Log-keeping was the last thing on his mind as the bunker erupted in noise and confusion. Reflecting on his treatment by the establishment, Petrov observed: "[T]he Commission [of Inquiry] was looking for scapegoats …" (Petrov cited in [20]).

Petrov, attacked by the Russian establishment, was celebrated by the international community. The Union of Concerned Scientists [31, 2] observed: "[T]he strongest, and one of the few, safety links in the chain was the judgment of the officer in command of the early warning centre [Petrov]". In 2013, Petrov was awarded the Dresden Peace Prize.

When Petrov passed away, his death went unannounced in Russia for four months [29] (Fig. 4). A vindictive snub? The independent-minded *Moscow Times* [21] observed: "Petrov died quietly at his Moscow home on May 19, 2017. Not a single media outlet reported on his death until last week [the week commencing September 10, 2017]". Vladimir Putin, the ex-KGB man, was President of Russia at the time of Petrov's death.

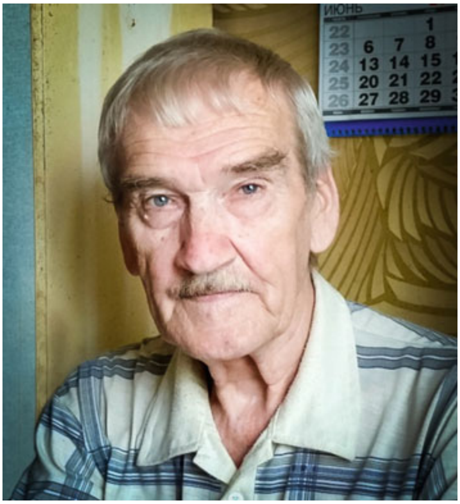

**Fig. 4** Lieutenant-Colonel Stanislav Petrov, celebrated by the enlightened, sidelined by the unenlightened, photographed in his modest apartment [35]

## 3 Conclusions

A number of conclusions can be drawn from the 1983 War Scare:

- systems that provide opportunities for human intervention are more reliable than systems that do not. Had the Soviets implemented a fully-automated system, the false-positive produced by the errant satellite would have automatically triggered a war alert at the highest levels of government that could have ended with the USSR launching its ICBMs against the US
- where opportunities for intervention are provided, care must be taken to ensure that those entrusted to decide whether or not a system is operating within limits are able to think independently, rationally and fearlessly. Operators with authoritarian mindsets are a liability. Such individuals are latent errors
- where opportunities for intervention are provided, care must be taken to ensure that those entrusted to decide whether or not a system is operating within limits possess the knowledge required to make informed judgments. Such knowledge must include an awareness of known weaknesses (latent errors) and work-arounds—informal routines developed by operators to compensate for system deficiencies. Fortunately for humanity, Petrov was very aware of the Oko system's latent errors: "He knew the limitations of a system he had helped to install" [11, 199]
- technology is fallible. As demonstrated by the Boeing737MAX-8 accidents, the curtailment of OFT1, the autonomous vehicle accidents, the 1980 NORAD near-miss and the 1983 War Scare, systems can host latent errors that may, via socio-technical processes such as safety migration [24, 25, 27], reactive patching [32] and emergence [18], and systemic interactions with a fluid social, economic, political and natural environment, mutate into active errors (faults), causing near-misses, incidents and accidents.

Those entrepreneurs who stand to make fortunes out of the latest automated devices would rather we forget such failures. Politicians whose laws and spending nurture the automation drive would rather we forget such failures. News of failure unsettles the markets and frightens investors.

The conscientious have a duty to remind the public that, as Arlindo Oliveira explains, technology can never be made 100% reliable. Given this fact, it is essential that designers provide human operators:

- opportunities to verify that systems are operating within limits
- opportunities to intervene if a system is operating unsafely.

To be able to intervene successfully, the operator must be provided adequate, high-fidelity data on system status and performance. Further, s/he must have the knowledge and skills needed to make informed judgments. Finally, s/he must have the psychological strength to think and act independently for the public good.

## References

1. Aksenov P (2013) Stanislav Petrov: the man who may have saved the world. https://bbc.co.uk/news/. Accessed 20 May 2021
2. Bainbridge L (1983) Ironies of Automation. Automatica 19(6):775–779
3. Bennett SA (2020) The disappearing pilot. A critique of distributed crewing—the necessity of a two-pilot flight-deck. The Log, Summer, p. 27. http://portfolio.cpl.co.uk/The-Log/2020-summer/cover/. Accessed 24 May 2021
4. Billings CE (1997) Aviation Automation: the search for a human-centred approach. CRC Press, Boca Raton FLA
5. British Broadcasting Corporation (2018) Uber halts self-driving car tests after death. https://bbc.co.uk/news/business/. Accessed 24 May 2021
6. British Broadcasting Corporation (2019) Tesla Model 3: Autopilot engaged during fatal crash. https://bbc.co.uk/news/technology/. Accessed 24 May 2021
7. Burdick E, Wheeler H (1962) Fail-Safe. McGraw-Hill, New York NY
8. Burriss L (2019) Slouching toward nuclear war: co-orientation and NATO exercise Able Archer 83. Int J Intell Secur Public Affairs 21(3):219–250
9. Davenport C (2020) NASA shows it's lost confidence in Boeing's ability to police its own work on Starliner space capsule. https://www.seattletimes.com/business/boeing-aerospace/nasa-shows-its-lost-confidence-in-boeings-ability-to-police-its-own-work-on-starliner-space-capsule/. Accessed 2 Nov 2020
10. Dibb P (2013) The nuclear war scare of 1983. How serious was it? Australian Strategic Policy Institute, Canberra
11. Downing T (2018) 1983: The World at the Brink. Little, Brown Book Group, London
12. Fischer B (1997) A Cold War Conundrum: The 1983 Soviet war scare. Central Intelligence Agency, Centre for the Study of Intelligence, Washington DC
13. Fiske S, Taylor S (1984) Social Cognition. Random House, New York NY
14. Fry H (2018) Hello World: How to be human in the age of the machine. Doubleday, New York NY
15. Green R, Muir H, James M, Gradwell D, Green RL (1996) Human Factors for Pilots, 2nd edn. Ashgate Publishing Ltd., Aldershot
16. Herena P (2011) The principle of fail-safe. https://www.aiche.org/chenected/2011/02/principle-fail-safe/. Accessed 26 May 2021
17. Hoffman D (1999) I had a funny feeling in my gut. https://washingtonpost.com/. Accessed 20 May 2021
18. Hollnagel E, Wears RL, Braithwaite J (2015) From Safety-I to Safety-II: A White Paper. University of Southern Denmark, Copenhagen
19. Lewis P, Williams H, Pelopidas B, Aghlani S (2014) Too Close for Comfort. Cases of near nuclear use and options for policy. The Royal Institution of International Affairs, London
20. Libak A (2004) Nuclear War: Minuteman. https://brightstarsound.com/world_hero/weekendavisen.html/. Accessed 30 May 2021
21. *Moscow Times* (2017) Stanislav Petrov, who saved the world from nuclear holocaust, died in May. https://www.themoscowtimes.com/2017/09/18/stanislav-petrov-died-in-may-a58967/. Accessed 31 May 2021
22. Oliveira A (2018) Making algorithms work for us. Nat Electron 1:487
23. Perrow C (1984) Normal Accidents. Living with high-risk technologies. Basic Books, New York NY
24. Rasmussen J (1997) Risk management in a dynamic society: a modelling problem. Saf Sci 27(2–3):183–213
25. Rasmussen J (1999) The concept of human error: is it useful for the design of safe systems? Saf Sci Monit 3(1):1–3
26. Reason JT (1990) Human Error. Cambridge University Press, Cambridge