DIGITAL WEAPONS OF MASS DESTABILIZATION

The Future of Cyber and Weapons of Mass Destruction

Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction

A Threatcasting Lab Report

ASU

DIGITAL WEAPONS OF MASS DESTABILIZATION

The Future of Cyber and Weapons of Mass Destruction

Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction

Technical Report by Brian David Johnson, Jason C. Brown, Josh Massad

The Threatcasting Lab is supported by

PARTICIPANTS

Dr. Gary Ackerman, Center for Advanced Red Teaming, University at Albany
Dr. Karyn Apfeldorf, Arete
Markus Binder, National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland
Ronald Breiger, University of Arizona
Patrick Concannon, University of Florida Genetics Institute
Rachel Costello, Entrepreneur in Residence, Office of Innovation & Commercialization, UC San Diego
Joel Dawson, Oak Ridge National Laboratory
Wilson F. Engel, III, Ph.D., Science Fiction Writer
Madhav Erraguntla, Knowledge Based Systems, Inc.
Jon-Paul Flodin
Christian Haliday
Nyle Hamidi
A. Kavanaugh
Benjamin C Kirkup, Naval Surface Warfare Center, Indian Head
Elizabeth Kistin Keller, Sandia National Laboratories
Dr. Stephanie Koorey, Australian National University
Marvin Leal, U.S. Army Network Enterprise Technology Command
Rhiannon Leal, Arizona State University
Heather Meeks, Defense Threat Reduction Agency
Alex Miller, GRIMM
Dr. Felicity Millman, 3A Institute, Australian National University
Eric Popiel
Dr. Lesley Seebeck, Australian National University
Nathan Shedroff, California College of the Arts
Dr. Steve Sin, START, University of Maryland
Dr. Peter Vandeventer, Defense Threat Reduction Agency
Rhyner Washburn, START, University of Maryland
Steven Winn, Arizona State University
Michael Woudenberg, Lockheed Martin
Whitney Lennon, Partnered Innovation
Anonymous

ASU THREATCASTING LAB TEAM

Brian David Johnson	Director
Cyndi Coon	Chief of Staff
Natalie Vanatta	Senior Advisor to the Lab
Jason Brown	Ph.D. Student

Arizona State University Threatcasting lab

The Threatcasting Lab at Arizona State University serves as the premier resource for strategic insight, teaching materials, and exceptional subject matter expertise on Threatcasting, envisioning possible threats ten years in the future. The lab provides a wide range of organizations and institutions actionable models to not only comprehend these possible futures but to a means to identify, track, disrupt, mitigate and recover from them as well. Its reports, programming and materials will bridge gaps, and prompt information exchange and learning across the military, academia, industrial, and governmental communities.

MOVING FROM MASS DESTRUCTION TO MASS DESTABILIZATION

THE FUTURE OF CYBER AND WMD

In the coming decade, a global proliferation of networked technologies will widen the cyber threat landscape. Pairing new and unforeseen cyber vulnerabilities with weapons of mass destruction (WMD) increases the secondary threats that cyber attacks bring and also necessitates a shift in definitions. WMD will become weapons of mass destabilization, allowing adversaries to gain strategic advantage in novel ways. Altering this definition provides clarity and specific actions that can be taken to disrupt, mitigate and recover from this combined threat. Additionally, a new class of Digital WMD (DWMD) will emerge, threatening military, government, and civilian targets worldwide. These combined and new threats will require the expansion of current defensive or mitigation activities, partnerships, and preparation.

Future Threats:

- **Cyber-aided WMD:** This is a time-phased threat can be further segmented into four additional categories:
  - Creating opportunity before the threat
  - Giving assistance during the threat
  - Providing amplification after the threat
  - Spreading falsification creating the threat
- **A Biological Hybrid:** Integrating traditional biological WMD with digital design components and a cyber attack
- **Weapons of Mass Destabilization:** Cyber and digital effects necessitate a new and expanded definition for WMDs

Conditional Indicators:

- **Ever Expanding Failures in Communication and Trust**
- **Mass Population Relocations**
- **Persistent Lack of Detection Capabilities**
- **Continued Failure of Responsibility**

Actions to be Taken:

- **Know Thy Enemy**
  - The Coming Increasing Complexity of Threat Actors
- **Necessary Strategic Mindset Shifts**
  - From Mass Destruction to Mass Destabilization
  - From Threats to Vulnerabilities
- **Prep for Atrocities Before they Happen**
- **Design Complex Systems for Security**

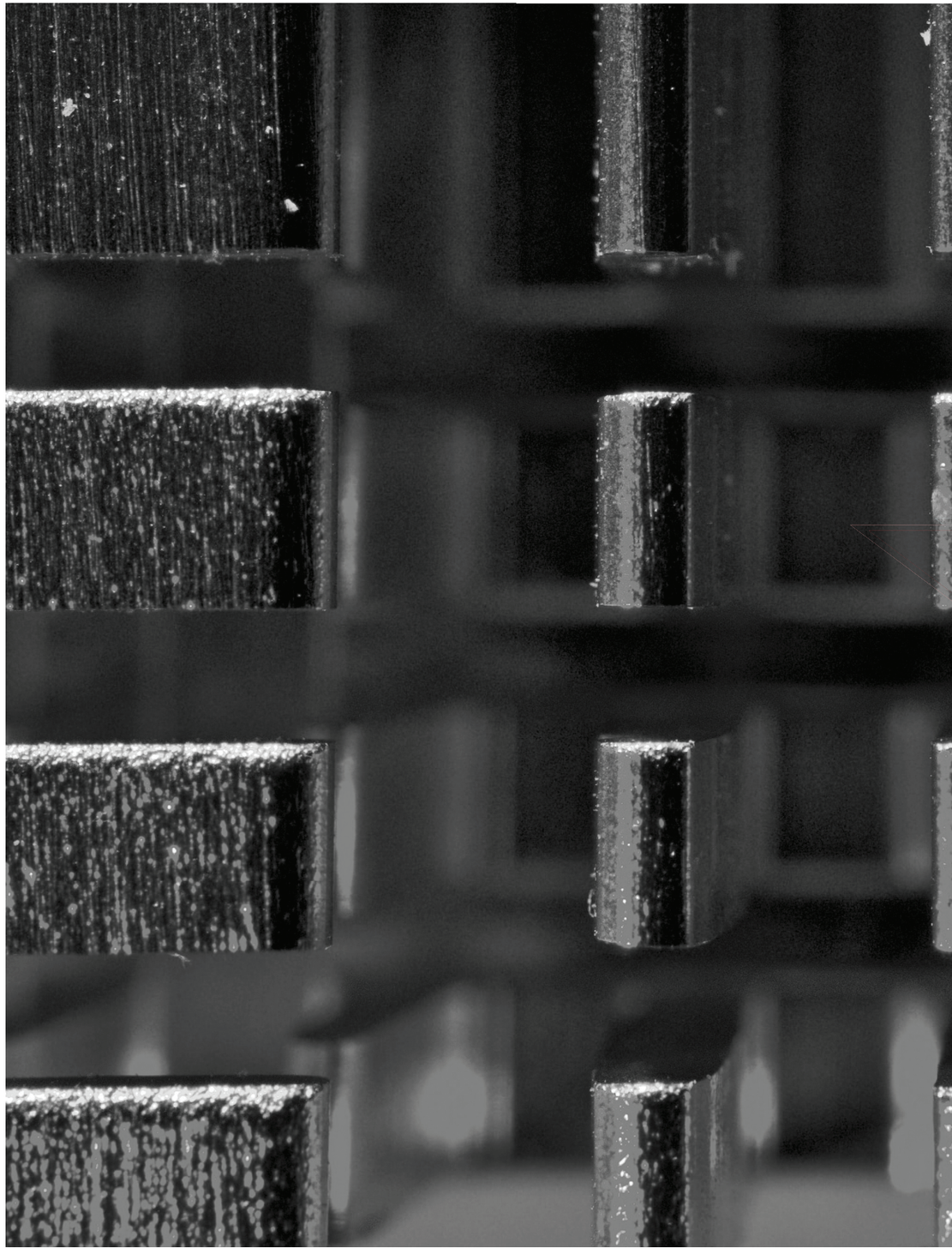
TABLE OF CONTENTS

RESEARCH OBJECTIVE

Both state and non-state adversaries have indicated a growing willingness to employ a wide range of offensive cyber tools for achieving a varied set of political and military ends. These operations are becoming increasingly sophisticated in nature, and steadily more integrated into adversary military doctrine, strategies, plans, and operations that already incorporate and integrate conventional and unconventional weapons, to include WMD. These developments necessitate an assessment of the potential nexus between offensive cyber operations and WMD and the implications for Countering WMD (CWMD), one of the Defense Threat Reduction Agency's (DTRA) missions.

The results of the Threatcasting process and workshop provide DTRA with a new and innovative perspective on the broad range of possible and potential threats at the intersection of WMD and Cyber weapons. We explore these threats in depth and also outline the possible 2nd- and 3rd-order effects that might come from them. Additionally, the results explore specific steps that can be taken today to disrupt, mitigate and recover from these threats.

The output of Threatcasting also identifies not only actions that can be taken by DTRA and other parties but also events, technologies and changes that could happen over the next decade that will indicate whether we are moving toward or away from the potential threats occurring.



INTRODUCTION TO THREATCASTING

Threatcasting is a conceptual framework used to help multidisciplinary groups envision future scenarios. It is also a process that enables systematic planning against threats ten years in the future.

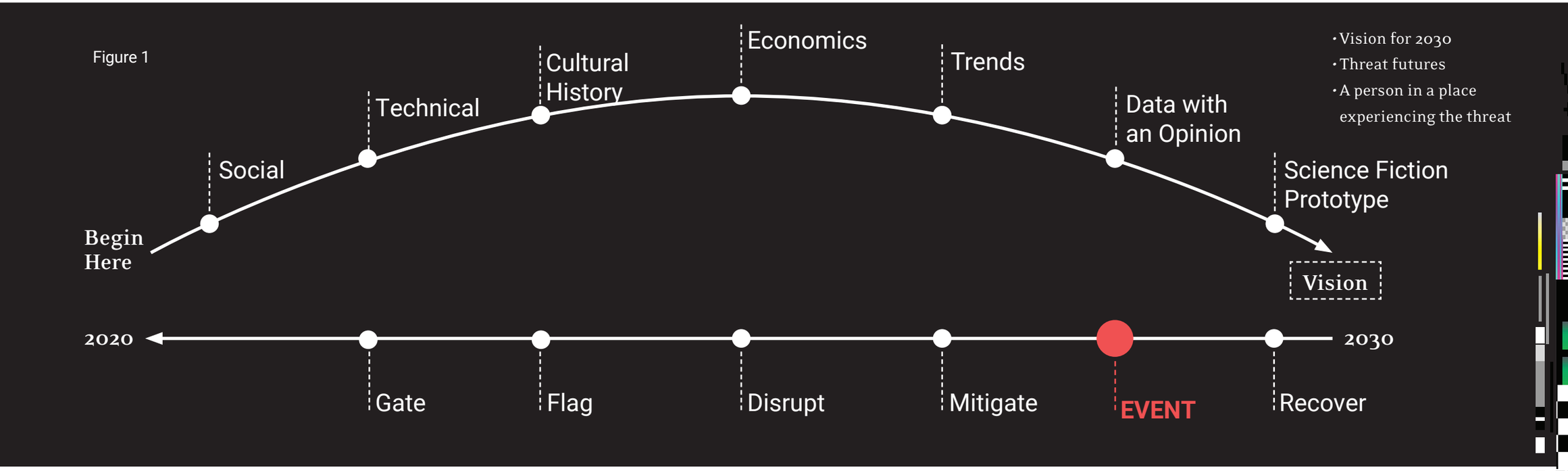
Utilizing the threatcasting process, groups explore possible future threats and how to transform the future they desire into reality while avoiding undesired futures.

Threatcasting is a continuous, multiple-step process with inputs from social science, technical research, cultural history, economics, trends, expert interviews, and science fiction storytelling. These inputs inform the exploration of potential visions of the future.

A cross-functional group of practitioners gathered for two days in February 2020, to create models of WMD threat futures. The outcome is the beginning of a set of possible threats, external indicators and actions to be taken. It is not definitive but does give the organization a starting place. Drawing research inputs from a diverse data set and subject matter expert interviews, participants synthesized the data into workbooks* and then conducted three rounds of threatcasting sessions.

These threatcasting sessions generated approximately 45 separate scenarios, each with a person, in a place, experiencing their own version of the threat. After the workshop concluded, futurists at the ASU Threatcasting Lab methodically analyzed these scenarios to categorize and aggregate novel indicators of how the most plausible threats could materialize during the next decade and what the implications are for “gatekeepers” standing in the way of the threats.

Figure 1



DEFINITIONS

Before we explore future threats at the intersection of cyber and WMDs, it is important to understand current definitions and directives for these two areas. Unfortunately, clear and specific documentation and definition of these terms does not exist. Multiple sources provide various perspectives on the terms.

For the purposes of this report, we have pulled together a consensus and a working definition to discuss the future of WMDs as well as the intersection of cyber with WMDs and any novel threats that might emerge. These working definitions are meant to serve the report and are not meant to definitively define the terms.

Weapons of Mass Destruction

Definition 1:

Weapons of mass destruction (WMDs) constitute a class of weaponry with the potential to, in a single moment, kill millions of civilians, jeopardize the natural environment, and fundamentally alter the world and the lives of future generations through their catastrophic effects.[1]

Definition 2:

Chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties.[2]

Definition 3:

a) any destructive device as defined in section 921 of this title; b) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors; c) any weapon involving a biological agent, toxin, or vector (as those terms are defined in section 178 of this title); or d) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.[3]

Working Definition:

Collectively these perspectives define a WMD as a weapon that is:

- Chemical, biological, radiological, nuclear, or explosive[4] in nature
- Intended to create mass casualties, jeopardize the environment and fundamentally alter the world

[1] United Nations
[2] Department of Defense (Joint Publication 1–02)
[3] U.S. Code
[4] This includes the 'E' in CBRNE. Improvised Explosive threats on a mass scale (e.g. forcing planes to crash is a type of improvised explosive device)

DEFINITIONS

Cyber and Cyberspace

Definition 1:

"Cyber: Of, relating to, or involving computers or computer networks (such as the Internet)."[5]

Definition 2:

"Cyberspace. A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[6]

Definition 3:

Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals.[7]

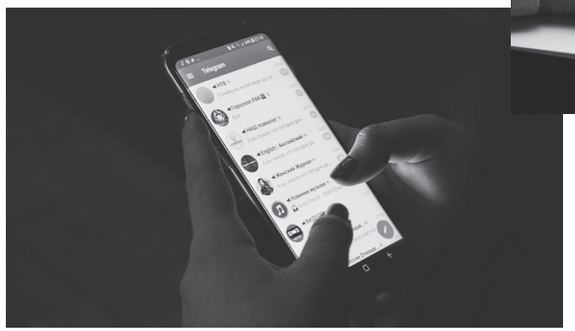
Working Definition:

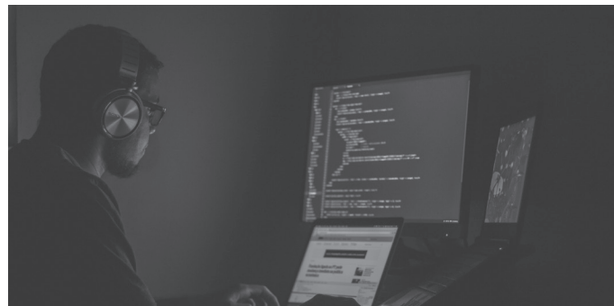
Collectively these perspectives define Cyber and Cyberspace as involving:

- Computer systems
- Tele-communications networks
- Data
- The Internet
- Embedded processors and controllers

Conclusion

These working definitions give a starting point to define the threat space and identify any novel potential and possible threats that could fall within these parameters and also land outside the boundaries, necessitating an expansion of the definitions.





[5] Merriam-Webster dictionary.
[6] Department of Defense. (2018, June 8). Cyberspace operations (Joint Publication 3-12).)
[7] International Association of Chiefs of Police

CYBER AIDED WMD FRAMEWORK

In a world where cyber activities are dominating social, economic, and national security interactions, there are increasingly new ways to open windows to other vulnerabilities. This includes the use of WMDs to further disrupt world order.

The Cyber-aided WMD framework includes four subcategories, segmented into three time-phased sections: Before, During, and After the WMD threat appears, as well as a Ubiquitous subcategory that emphasizes falsification of a WMD threat during any phase. In other words, the cyber-aided WMD framework looks at how cyber effects appear before, during, and after a WMD threat and how falsification during all phases changes how the threat is perceived.

The purpose of the framework is to categorize a range of possible and potential threats at the intersection of cyber and WMDs so that a possible set of actions and indicators can be defined to disrupt, mitigate and recover from them.

OPPORTUNITY - BEFORE THE THREAT

"Opening a Window to a Vulnerability"

The first time period for a cyber aided threat occurs before the WMD attack occurs. These cyber attacks will take advantage of vulnerabilities in security systems that already exist. Hackers (a digital attacker) will purposefully create and penetrate cyber defenses allowing bad actors (a physical attacker) to gain access to important infrastructure to create or open a window of opportunity to employ a traditionally defined WMD. In some cases, the digital actor and the physical actor might be the same person or may support the same group. In other cases, a digital attacker might sell their compromised data to another organization and facilitate a physical attack without being part of the same team.

Although this category of threat can encompass every attack against cyber-controlled critical infrastructure (e.g. energy, financial, or the health service sectors), the novel component of this threat are the situations when Bad Actors exploit cyber vulnerabilities to employ a traditional CBRNE WMD and then "steps aside".

> *Hackers (digital attackers) gain cyber control of advanced small, trailered nuclear power generator systems that leads to a localized meltdown.*[8]

> *Hackers gain external control of a fleet of automated passenger planes via a cyber exploit and cause all planes to simultaneously crash.*[9]

[8] See Appendix 3: Red Pawn 2
[9] See Appendix 3: Yellow Pawn 3

ASSIST-DURING THE THREAT

“A New Force Multiplier”

The Assistance based threat identifies a cyber or digital attack that will assist a traditional WMD in the midst of being deployed. The most powerful use is having the digital attack enable a chain reaction of physical and social effects caused by the WMD.

> *Hackers (digital attackers) lock down 911 and emergency service dispatch systems with ransomware after a radiological device is detonated by Bad Actors (physical attackers) in the U.S. capitol region.*[10]

AMPLIFY - AFTER THE THREAT

“If a WMD is deployed in the woods…”

The Amplify category of cyber aided effects occurs after the WMD attack and draws on a vast history of information warfare methodologies. This type of effect largely exploits news and social media in order to amplify the social disorder that would normally occur. The cyber component will serve to amplify or advertise the effects of the WMD attack more broadly. Further effects will be scenarios where actors, Good, Bad and Gray, engage in a rolling “blame game”, falsely or unable to identify attribution. This exposes the difficulties in attributing a WMD attack to the correct party.

> *A bioengineered virus transmitted through the chicken meat supply system will be blamed on Venezuela via a Russian misinformation program. The threat actor introduces a pathogen into the supply chain that will cause a local epidemic at the same time they are using social media to stoke racial tensions in different parts of the country.*[11]

FALSIFY - CREATING THE THREAT

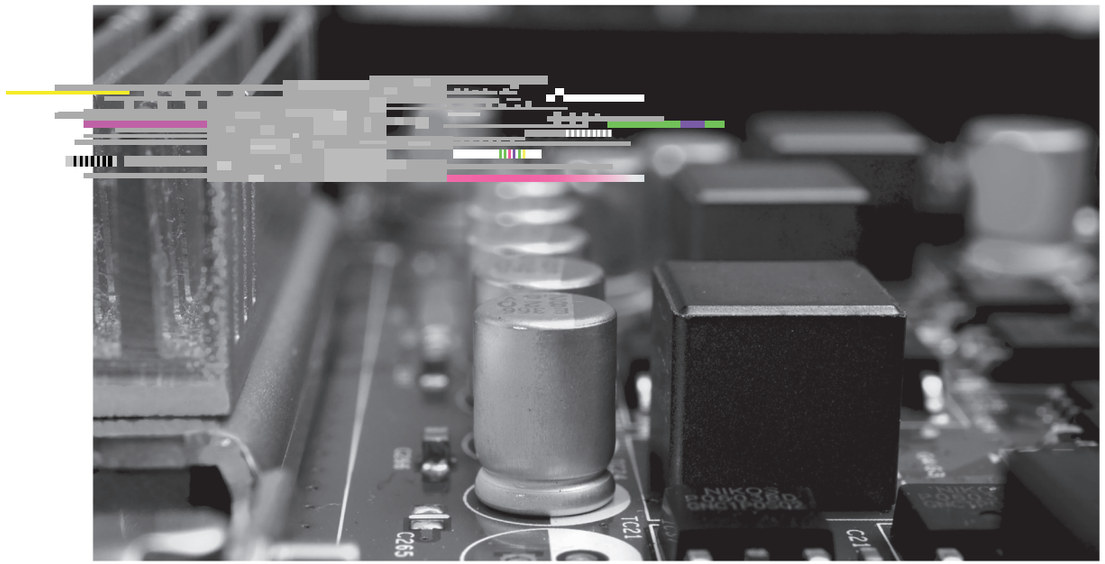
“When a WMD is not a WMD but becomes a WMD.”

The fourth category of effects defines a cyber attack that will falsely identify an action, natural event or disinformation campaign as a weapon of mass destruction. However, the public’s belief that a WMD has been used could bring about the defined effects of a WMD.

The fourth category of cyber aided WMD will strongly rely on social networking and the areas traditionally defines as cyber and cyberspace (Computer systems, Tele-communications networks, Data, The Internet, Embedded processors and controllers) to spread and leans heavily on the power of information disorder machines[12] so the adversary can gain an advantage.

Because the attack will be digital in nature, it will not in itself meet the current definition for a WMD, however the effects could meet the current definition. This incongruity pushes us to consider not only redefining the nature of a WMD to include “digital in nature” but also a reframing of the potential effects beyond a traditional WMD. This is further explored below under Future Threat: Digital Weapons of Mass Destabilization.

> *A major Smart City in 2030, with its highly connected suite of millions of Internet of Things devices, including radiological detection sensors, falsely sends out an “amber alert” that reports the detonation of radiological devices in the city and orders an immediate evacuation. Chaos and panic rapidly overwhelm evacuation routes, communication channels, and people's sense of civility as they attempt to escape the (non-existent) threat.*[13]



[10] See Appendix 3: Green Pawn 2
[11] See Appendix 3: White Pawn 1
[12] Johnson, B. ([2019]). Information disorder machines: Weaponizing narrative and the future of the United States of America. Arizona State University.
[13] See Appendix 3: Neon Yellow Pawn 2

THE BIOLOGICAL HYBRID

The Biological Hybrid future threat is a combination of a traditional biological WMD integrated with a digital design component and cyber attacks. Although this threat appears to have similar effects to those of a traditional biological WMD, new characteristics emerge from cyber capabilities of the data.

The nature of the digital design of biological weapons opens further complications and complexities to this attack vector. The lowering threshold for access to do-it-yourself CRISPR genetic manipulation labs and the computing power needed to develop new recombinant DNA models can be purchased for the low thousands of dollars. This threat will undermine trust systems in novel ways.

> *An adversary introduces a bioengineered virus into the vaccine supply chain destined for U.S. military facilities as a measure to bolster defenses against biological terrorism. A non-state actor develops this new virus from stolen 23andMe genetic data and attempts to target the largely white leadership of the U.S. strategic (nuclear) force to cause a disruption in command, control, and response capabilities of the nuclear force.*[14]

[14] See Appendix [3]: Neon Yellow Pawn 1

DIGITAL WEAPONS OF MASS DESTABILIZATION

A NEW DEFINITION.

A digital weapon of mass destabilization begins at the intersection of cyberspace and traditional WMDs, but requires us to consider how a digital or cyber attack(s) could create mass casualties, jeopardize the environment, and fundamentally alter the world in similar scope and consequence to the effects of a WMD. However, the digital nature of a digital WMD means that it falls outside of the current understanding that a WMD is chemical, biological, radiological, nuclear, or explosive in nature and has destruction at its core.

These new effects suggest a revised definition of WMDs that expands the scope to include digital weapons, by recognizing their mass effect. Weapons of mass destruction can be expanded to a new class of Digital Weapons of Mass Destabilization (DWMD) to encompass the new digital or cyber nature of these weapons and their expanded effects. A DWMD may contribute to destructive endstates, but its primary nature is one of massive, highly consequential social, political, and economic destabilization.

THE DESTABILIZATION PRECEDENT - HISTORIC EXAMPLES.

The definition of a DWMD is expanding to encompass the digital nature of a WMD and its expanded effects beyond the traditional "destruction". The notion that a weapon of mass destruction could be seen as a weapon of mass destabilization is not without precedent.

The destabilizing aspect of this new definition does not require lives lost in the initial attack. Therefore, there is now room to accommodate cyber-attacks and secondary effects. The objective of destabilization is not new in general and does have some historical reference with mass effect.

The cyberattack instigated by the Russian military in 2017 against Ukraine was disguised as a ransomware attack as "part of the Kremlin's ongoing effort to destabilize Ukraine."[15] The victims' computers were locked down with a message to pay or lose their data. However, the purpose of this cyberattack was "meant to paralyze, not profit."[16] The virus shut down "six power companies, two airports, more than 22 Ukrainian banks, ATMs and card payment systems in retailers and transport, and practically every federal agency. The government was dead, surmmarizes Ukrainian minister of infrastructure Volodymyr Omelyan."[17]

On a global level, this weapon caused destabilization through the largest shipping company in the world, Maersk.[18] The company only had one computer in Ukraine which was enough to penetrate the company systems and shut down their global shipping operations causing perishable goods to be endangered and miles of traffic jams of semi-trucks waiting at ports around the world to haul the goods from Maersk. This event "resulted in the most destructive and costly cyberattack in history, causing billions of dollars in damage across Europe, Asia and the Americas."[19]

"Mass destruction extends beyond the immediate victims of those weapons classified as WMDs…when it comes to inflicting mass destruction, the cascading effects of population displacement and despair are not merely collateral damage—they are the primary strategic objective."[20] In 2013 the Assad regime in Syria used the WMD sarin gas killing 1,500 of its civilians. Due to the attacks in Syria, there was mass displacement causing citizens to become refugees seeking asylum anywhere they could reach. Millions of Syrians looked for somewhere else to live besides Syria. This sudden migration caused compounding and complex problems for the surrounding countries and into Europe. "While parts of Syria are being depopulated, the massive displacement is destabilizing the region and beyond."[21] The two examples are vastly different in their technological prowess, however, each was able to destabilize on a regional and to some extent, on a global level.

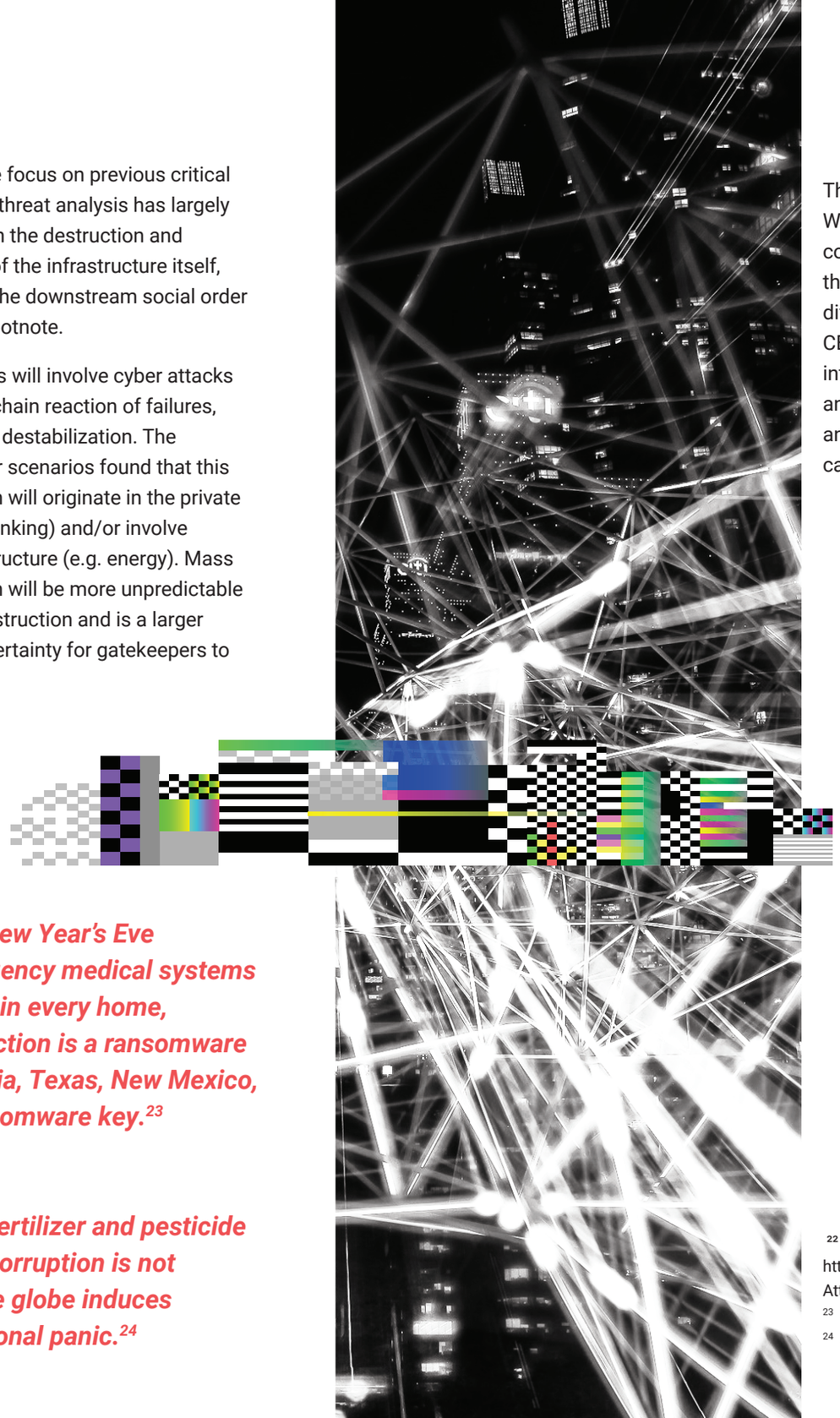
[15] U.S. Department of Justice. (2018). Report of the Attorney General's Cyber Digital Task Force. p. 25.
[16] Ibid
[17] Greenberg, A. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[18] Ibid.
[19] U.S. Department of Justice. (2018). p.25.
[20] The Soufan Center. (2018, July 10). TSG IntelBrief: Weapons of mass destruction, displacement, and despair. https://thesoufancenter.org/tsg-intelbrief-weapons-of-mass-destruction-displacement-and-despair/
[21] Ibid.

FUTURE DWMD IN THE WIDENING ATTACK PLANE.[22]

Cyber security experts for years have worked tirelessly to consider the many ways cyber vectors can affect critical infrastructure. It is widely believed that electrical grids, water supply systems, banking and economic systems, and other key infrastructure nodes have become increasingly vulnerable to cyber attacks. Digital compromise of SCADA (Supervisory Control And Data Acquisition) controls at a dam could lead to floodgate failures, causing massive downstream flooding.

We believe the focus on previous critical infrastructure threat analysis has largely narrowed in on the destruction and compromise of the infrastructure itself, while leaving the downstream social order effects as a footnote.

Future DWMDs will involve cyber attacks that set off a chain reaction of failures, causing mass destabilization. The majority of our scenarios found that this destabilization will originate in the private sector (e.g. banking) and/or involve critical infrastructure (e.g. energy). Mass destabilization will be more unpredictable than mass destruction and is a larger source of uncertainty for gatekeepers to plan for.



The post analysis found that every digital WMD aimed at destabilization also contains an element of “Opportunity” from the cyber aided WMD framework. The difference is that there is no traditional CBRNE attack that accompanies the cyber intrusion. The digital weapon itself causes an equivalent or greater level of destruction and destabilization than a traditional WMD can cause.

A Mexican drug cartel capitalizes on the U.S. New Year’s Eve countdown celebration and the strain on emergency medical systems to infect unsecured internet of things products in every home, business, and building in the country. This infection is a ransomware that demands the return of portions of California, Texas, New Mexico, and Arizona to Mexico in exchange for the ransomware key.[23]

Hackers corrupt the sensor data that controls fertilizer and pesticide spraying in fully autonomous farms. The data corruption is not noticed until widespread crop failure across the globe induces increasing food supply shortages and international panic.[24]

[22] Johnson, B. ([2017]). The widening attack plain. Arizona State University. http://threatcasting.com/wp-content/uploads/[2017]/[03]/A-Widening-Attack-Plain.pdf

[23] See Appendix 3: Black Pawn 3

[24] See Appendix 3: Denim Blue Pawn 3

Analysis of the raw data and emerging themes from Threatcasting workshops revealed a number of threat indicators, or flags, of cyber aided WMDs, the Biological Hybrid and DWMDs.

CONDITIONAL INDICATORS AND FLAGS

The implications from the threat findings reveal a range of flags, or events and realized situations, identified directly and indirectly from the threat future data that give us specific areas to progressively monitor for possible threat futures. Marshall, et al.,[25] propose that the progression of disorder is always subjective and therefore, the flags that forecast the imminent threat, may also be subjective.

DEFINITION: FLAGS

The Threatcasting process not only maps possible and potential threats 10 years in the future but attempts to identify the flags (indicators) that serve as signals or trends indicating a specific threat future is underway. Sometimes referred to as "signals,"[26] these flags can give an early warning that a possible and potential threat future is in-flight or beginning to form. Often, flags are sequential with less apparent precursors already in effect, and the more alarming flags still over the horizon. It remains unsolved how best to monitor them at scope and scale.

The following flags are grouped into the threat areas as well as specific subcategories or domains so that these can be monitored for indicators that the flags have happened. These subcategories are designed to help practitioners utilize and apply the flags to their work. They are not meant as a definitive classification.

Many flags can be categorized in multiple domains (e.g. technical, cultural, social, economic, regulatory, etc.). Each of the flags below is a micro-indicator that the threats outlined in this report are beginning to emerge. Often flags will build off each other, giving DTRA multiple early stage indicators to prepare for the threat.

CONDITIONAL INDICATORS

The post analysis revealed four overarching conditions or indicators that the threat futures -- cyber aided WMDs, the Biological Hybrid, and DWMDs -- are beginning to materialize. Each of these four provides heightened conditions in which all three threat areas become more possible and likely. In this section, we also use the term additive flags, which are threat indicators that build from one to the next. Often, these flags are dependent upon the success of a previous flag emerging. Occasionally, a precursor flag might appear from a different sector (e.g. a technological advancement) that perpetuates through other sectors, such as politics. These "flags" are meant to be visible signals that the conditions are developing for specific future threats.

[26] Webb, A. (2016). The signals are talking: Why today's fringe is tomorrow's mainstream. PublicAffairs.

Ever Expanding Failures in Communication and Trust.

Recovery from a WMD requires resilient and redundant communication platforms that allow for the two-way exchange of information to/from the population and the government. Communication also requires trusted sources. In the future, Information Disorder Machines will put more people at risk of the secondary and tertiary effects of a WMD because of untrustworthy information, untrustworthy sources, or purposeful manipulation of data.[27] This erosion of communication and trust will become a fertile ground to sow the seed not only of cyber aided WMDs and Biological Hybrids but more importantly the landscape necessary for DWMDs.

ADDITIVE FLAGS

Information Disorder and National Security

- Expansion of unchecked information disorder with a nebulous goal of sensationalization, profit, divisiveness - not a specific issue or group
- Growing skepticism and balkanization of truth that moves beyond civil debate
- Consumer-grade (non state or Corporate funded) use of artificial intelligence and bots to target in-country citizens and groups
- Expansion and acceptance of generalized anger, anxiety and frustration that spreads across a broad range of topics (not specific)
- Massive, systemic, and generalized social and cultural divides cause increased chaos and uncertainty[28]

Digitally Enabled Lone Wolves Coalesce

- Ransomware as a Service blurs the line between developers and attackers, lowering the barrier of entry for non-state funded threat actors
- “Leaderless resistance” movement of extremists with no precursor crimes begin to align
- Rumors/Confirmation of WMD acquisition by non-state sponsored groups
- A consolidated cyber “black swan” attack locks out emergency communication capabilities in conjunction with a WMD attack[29]

Infrastructure: Digital Advancement and Social Vulnerabilities

- Increased industrial and local governmental adoption of automated systems (IoT, industrial IOT, Smart Cities, 5G) surpasses respective security systems and analog failsafes
- Local regulation and coordinated security efforts fail
- Post 2020 reduction in neighborhood grocery stores
- Increasing dependency and optimization of just-in-time resources & food delivery
- External hack of smart city food storage & distribution leads to sudden food shortage[30]

[27] Johnson, B. ([2019]). Information disorder machines: Weaponizing narrative and the future of the United States of America. Arizona State University.
[28] See Appendix 3: Denim Blue Pawn 1
[29] See Appendix 3: Green Pawn 2
[30] See Appendix [3]: Grey Pawn 3

Mass Population Relocations.

Indicators of a population movement away from urban centers to avoid the problems associated with concentrating many people in a small space when exposed to biological attacks.[31] This “deurbanification” or “white (collar) flight” changes how adversaries will consider the extent of mass in a biological WMD. The ability (or inability) of certain advantaged groups to seek suburban or near-rural geographies also emphasizes who might be at greater risk for biological vectors that require higher levels of human interaction to spread and reach the mass level of effect.

ADDITIVE FLAGS

White (collar) Flight

- 2020 pandemic changes workflow and culture; increased development and reliance on remote working capabilities
- Policy to forgive trillions in student debt frees millennials to consider greater rates of home purchases in the U.S.
- Post 2020 recession and pandemic fall out push city infrastructures to crumble
- Surge in millennial suburban and near-rural home building & buying leaves urban centers concentrated with lower income and older populations[32]
- Bio-engineered virus attacks concentrate on under served communities (due to population densities), giving impression of being targeted

Weaponizing Infrastructure

- Economic fallout from 2020 pandemic shutters several industrial control suppliers, leaving a (near) sole-source manufacturer that can produce replacement parts for aging floodgate control systems in dams
- Continued urbanization (mega cities) condenses the population and strains water, electricity, trash, and housing infrastructures[33]
- Overdue repairs on infrastructure (e.g. dams) rushed to finish without sufficient security checks in place
- Hack on compromised infrastructure control systems exposes “weaponization” of dam (floodgates remotely controlled) threatening downstream mega city[34]

[31] See Appendix 3: Hot Pink Pawn 1
[32] Sharf,S. (2019, July 8). Yes, millennials really are buying homes. Here’s how. Forbes. https://www.forbes.com/sites/samanthasharf/2019/07/08/yes-millennials-really-are-buying-homes-heres-how/
[33] United Nations Department of Economic and Social Affairs (2018, May 16). 68% of the world population projected to live in urban areas by 2050, says UN. https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html
[34] See Appendix 3: Green Pawn 3

Persistent Lack of Detection Capabilities.

The rise of do-it-yourself bioengineering threats as well as the growing capability for sophisticated, one-off and zero-day cyber exploits will complicate the rate of detection, attribution, and proper response to emerging bio- and cyber-enabled threats. Understanding how current sensor and detection capabilities might be bypassed could also enable the spread of radiological material.[35]

Expanding the spectrum of "detectability" might include the ability to track the spread of databases of information or the ability to sense intrusions into IoT-enhanced Smart Cities. The persistent lack of detectability also hinges on technology advancements, laws, and social norms required to enable contact tracing and detection of "patient zero" in biological and cyber attribution.

ADDITIVE FLAGS

Rogue Food System Attack

- Low-cost home genetic manipulation labs enable the spread of hobbyist genetics
- Unexplained animal deaths in rural areas caused by extremist groups developing viruses that infect animals in countries without sufficient agriculture testing or safety policies
- Increased food insecurity leads to community blowback from lack of trust in local authorities and widespread hunger-based atrocities[36]

Genetic Fakes

- Hobbyist geneticists and entrepreneurs create an on-demand genetic "wellness" industry
- Dark web market established for untested genetic formulas that can be downloaded and "printed" at home
- Hackers take over advertisements for legitimate genetic wellness treatments and send buyers to sites delivering cheaper, dangerous, and untested versions; leaving consumers no way of verifying the accuracy and authenticity of these files until after the treatment is applied

Exploiting Data Security

- U.S. passes strict data privacy laws that criminalize the re-sale of personal information collected on smart phones and devices
- Health tracking apps and embedded personal health sensors detect new viruses and pathogens even when the user is asymptomatic
- Privacy laws prevent data from being shared, collated, and analyzed to identify outbreaks of new epidemics; patient zero is obfuscated under red tape and proprietary data storage
- Insider at a health data company leaks personal information data that can identify patient zero and emerging health trends, but everyone who touches and reports on the data is criminalized and indicted

[35] See Appendix 3: White Pawn 2, Turquoise Blue Pawn 2, Red Pawn 1
[36] See Appendix 3: Yellow Pawn 1

Continued Failure of Responsibility.

A WMD response such as outbreak containment, vaccine development or public safety measures are generally thought to be the responsibility of the government. Currently there exists little discussion on the responsibility of industry or academia in these situations. One exception is the research pipeline to make vaccines or the technology to detect threats.

Scenarios revealed much frustration on where and how much governments can and cannot affect, or control, the forces (social and otherwise) needed to mitigate and recover from a WMD. An inclusive discussion with industry, academia and all players is needed.

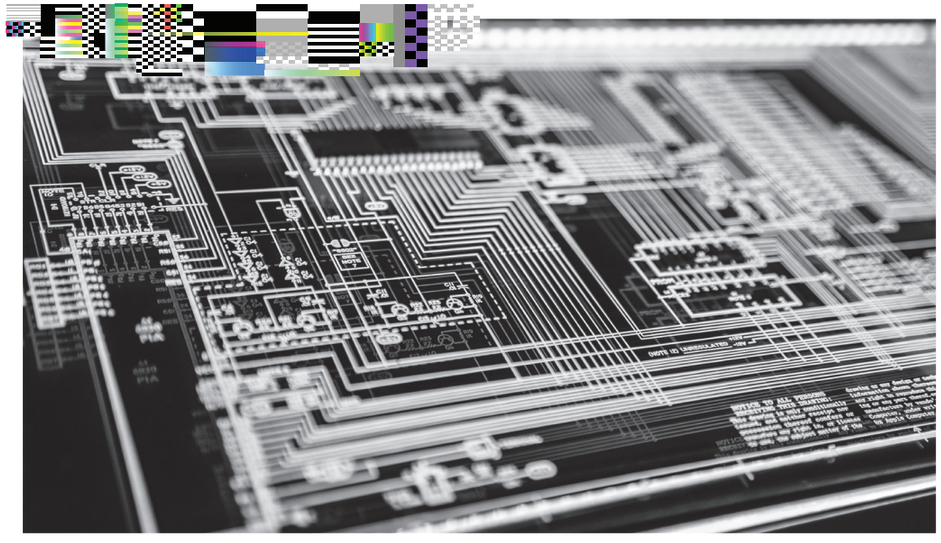
ADDITIVE FLAGS

Interstate Tensions Boil Over

- State and federal authorities disagree on timing, policies and efforts to mitigate emerging pandemic
- Hot spots of disease appear in certain cities and states with lesser restrictions - casualties rise to culturally “unacceptable” level
- Federal troops ordered to intervene, limiting interstate travel
- Interstate commerce restrictions create food insecurity in states that cannot grow own food
- Governors and state-first groups raise tensions

Deep Design Flaws

- Open source and collaborative projects, bioengineering and AI, become the norm for Gen-Z entrepreneurs
- AI, IoT, Smart Cities proliferate with little regulation or coordination
- Cities and state governments begin relying on cheaper, open source solutions
- Major cyber flaw corrupts hundreds of petabytes of government-funded data (e.g. agricultural, medical, IT, infrastructure, etc.)



The Threatcasting Workshop uncovered not only threats and flags but also actions that could be taken to help mitigate, disrupt, and/or recover from the threats. These actions constitute a "whole of society" approach to problem-solving and have been applied to specific domain areas where detailed steps can be taken. All these actions must be fluid to adapt and shape the future applications of technology.

STRATEGIC MINDSET SHIFTS

From Mass Destruction to Mass Destabilization

The intersection of cyber with WMD necessitates the shift to Digital Weapons of Mass Destabilization because the nature of the attack (digital) and the effect are not comprehended in the current WMD definition.

Additionally, the definition of mass effects as well as how adversaries could use a digital or cyber attack to create destabilization on a scale equal to or greater than the effects of a traditional CBRNE WMD. The private sector (banks, big businesses, food manufacturers, energy sector, etc) are likely early targets for a weapon of mass destabilization. This weapon will look to create a small attack that then begins a chain reaction, cascading effects across multiple sectors and ensuring political and social chaos.

From Threats to Vulnerabilities

As we change the emphasis of WMD from weapons of mass destruction to the concept of weapons of mass destabilization, we then can begin to shift our thinking from only identifying threats to also identifying the vulnerabilities that these threats match up with. It is critical that we now look inward to all the places that the threat could manifest.

This framing of threats and vulnerabilities is a common framework for describing risk. In this workshop, several groups considered risk to be the impact of an event times the probability of that event occurring. Other groups considered risk to be the impact of a threat multiplied by our vulnerability to that threat. Some of the difference comes down to an agreed upon measure of "mass," which isn't clearly defined, so that a WMD actually matters to the missions of DTRA.

One perspective might see that impact x probability is a better measure, where "impact" is the scale of how much destruction/disruption occurs. One difficulty with impact, especially in disruption through cyberspace, is that it is quite difficult to measure how much an influence operation changes, affects, or influences the minds and behaviors of target audiences and how much comes from exogenous forces. On the other hand, risk measures within DoD also consider the threat x vulnerability matchup, meaning, it's not worth the effort to shore up defenses against a threat where no vulnerability exists and, vice versa, it's not worth the effort to shore up defenses in an area of vulnerability if no threat exists. Risk is high only if impact, vulnerability, and threat actor motivation/capability are all significant.

Cybersecurity During a Pandemic

In the time between the threatcasting workshop in February 2020 and the publication of this report, the world experienced first-hand some of these imagined threats stemming from the intersection of a world-wide pandemic and cyber threats. The United States Cyberspace Solarium Commission identified additional flags that appeared during the COVID-19 pandemic, one of which did not appear in our threat futures. First, the Commission recognized the "need to digitize critical services and do so securely."[37] Several threat futures imagined the digital exploitation of emergency services and communication systems.[38] Our finding labeled "Design Complex Systems with Security in Mind" reflects the need for secure systems, especially those dealing with mass (official) communication and the restoration of essential services.

Second, the Commission identified a growing number of people working from home, which significantly changes the relationship between corporate network security and home-based network security. This introduces a new attack vector for cybercriminals that was not as prevalent before the pandemic. None of our threat futures considered this new flag.

Finally, the Commission identified an increase in fraud and financial exploitation due to the pandemic. Several of our threat futures identified opportunities such as fraud and financial blackmail as ways of disrupting order or to gain access to trusted systems for a more significant disruptive effect.[39]

[37] United States of America Cyberspace Solarium Commission. (2020, May). Cybersecurity lessons from the pandemic: CSC white paper #1. p. i.
[38] See Appendix 3: Green Pawn 2, Neon Yellow Pawn 2.
[38] See Appendix 3: Green Pawn 1, Red Pawn 3.

KNOW THY ENEMY

The Increasing Complexity of Threat Actors.

We do not fully understand the varied motivations of potential threat actors. In the next decade, threat actors are similar to those of today: state actors, criminal organizations, non-state actors, and opportunists with an agenda. The ease of entry into cyber-enabled attacks will continue to grow, allowing for those with a wide range of motivations to become potential threat actors. The ease of entry into do-it-yourself bioengineered threats will also continue to grow, especially when coupled with advancing artificial intelligence and the availability of genetic data stored online. This indicates a potential trend in the increase in novel viruses, bacteria, and other pathogenic vectors that easily fit within the umbrella of biological weapons. Scenarios were developed that explored these DIY viruses as weapons of mass destruction as well as weapons of increasingly narrow focus, targeting individuals or genetically similar phenotypes.

State actors will use cyber weapons to enable information disorder machines and widespread destabilization, but rarely did scenarios consider state actors directly attacking with a traditional WMD. This is likely due to current international agreements and norms against CBRNE effects and the relatively straightforward manner in which nation states are expected to respond to an attributed WMD attack.

However, this implies a need to better understand each threat actor. Investigating and considering the tools these actors have (whether commercial, open source, or proprietary) is only part of the equation. The nature of the threat actor and their motivations may also change how gatekeepers need to respond to future threats.

PREPARE FOR ATROCITIES BEFORE THEY HAPPEN

One continued theme discovered in the responses available to gatekeepers was a critique about not being prepared for events before they happened. Much of our infrastructure that can deal with WMDs is centered around recovery and to a lesser extent, mitigation (e.g. emergency medical systems, communication redundancy, policing, etc.) Glaring holes in the ability to anticipate the nature of emerging threats on a widespread scale and prepare for their eventuality was seen in many of the scenarios. Granted, it is expensive and laborious to fully prepare for every nuance of every eventuality in every city in the country, so some leniency is required in this critique. However, as this threatcasting workshop concluded, the nation was barely glimpsing the oncoming wave of COVID-19 epidemic responses required to maintain public safety and social order. The luxury of writing this report while living through and observing how different countries responded to this global pandemic reinforces the need to consider preparatory measures for the inevitable social, financial, and health atrocities that will occur during the next WMD event.

DESIGN COMPLEX SYSTEMS WITH SECURITY IN MIND

Many technologies, both on the hardware level, the software level, and even the human interaction level are not designed with security in mind. Many cyber systems, especially consumer systems, are designed for efficiency, productivity, ease of use, or market value. These types of design features are easy to hack and exploit. In fact, it is difficult to design a system that is equally efficient and secure. Until we design with security first, we are not designing safe systems.

A Safe Place is a Secure Place.

Continuing with a corollary of technology security, one of the recurring observations from our threatcasting scenarios was how differently people reacted when they felt secure in the ability to recover from or be protected from a WMD. Safety comes from a sense (both real AND perceived) of security. The types of safety-in-security concepts identified in our scenarios include the security of personal and genetic information; secure measures for development, transportation, and tracking of radiological materials; surety of reliable food and water supplies following a WMD event; and security in knowing information, news, and social media is not being purposefully manipulated.

SPECIFIC ACTIONS: GATEKEEPERS

This section reviews the actions gatekeepers in different domains (DTRA, government, academia, industry) can take to help disrupt, mitigate, or recover from the threats outlined in this report. The format follows the general framework of broad actions detailed in the section above. Data here is purposefully bulleted and raw, without additional discussion. This is because the Threatcasting Lab is providing recommendations that could occur given the imperfect sample of possible threat futures at the intersection of cyber events and WMD. We acknowledge gaps in our understanding and in the raw data gathered at the threatcasting workshop as well as gaps in understanding what tools are available to gatekeepers.

DTRA

Strategic Mindset Shifts

- Explore the shift from Destruction to Destabilization and its implications on strategy, planning and partnerships (Disrupt)
- Champion discussion across government, military, law enforcement, academia and business (and possibly the public?) (Disrupt)
- Develop doctrine and recommend policies for including cyber destabilization as a weapon of mass effect (Disrupt)
- Robust monitoring of cyber aided WMD activity, the Biological Hybrid and emerging effects from DWMD (Mitigate)
- Further iterate a recovery plan. (What does it mean to recover from a DWMD?) Explore network of partners and stakeholders (Recover)

Know thy enemy

- Develop partnerships and internal capability to map and explore a range of adversaries (Disrupt)
- Champion expanded networks to monitor adversarial activity in cyber and digital weapons with mass effect (Mitigate)

Prepare for Atrocities Before They Happen

- Develop internal experience to explore multiple scenarios at the intersection of cyber and WMD as a way to adjust culture and engage a broader set of partners (Disrupt)
- Develop expertise to inspect and monitor foreign cyber weapons development (Disrupt)
- Assist cities and states in wargaming future WMD threat scenarios (Disrupt)
- Explore and specify how the Biological Hybrid alters DTRA's mandate and partnerships (Disrupt/Mitigate)
- Explore how the Cyber Aided WMD Framework can be integrated into DTRA's mission (Disrupt/Mitigate/Recover)

Design Complex Systems with Security in Mind

- Encourage radiological detection in the food chain (Disrupt)
- Certification and registration guidelines that help secure the lowering bar to entry for bioengineered pathogens (Disrupt)
- Control the migration of biological precursors across borders (Disrupt)
- Train NGO personnel on how to detect WMD threats (Disrupt)

GOVERNMENT

Whole of government including federal, state, local and first responders:

Strategic Mindset Shifts

- Begin policy maker and leadership discussions around DWMD and Cyber aided WMD (Disrupt/Mitigate/Recovery)

Know thy enemy

- Develop standards and share incidents of indicators of compromise from ransomware incidents, especially related to biomedical hacking (Disrupt/Mitigate)
- Fund research projects to get to know the enemy (ethnographic and anthropological studies of our adversaries; fund legal research on cyber espionage versus extremism versus terrorism especially when incorporating DWMD or destabilizing cyber effects (Disrupt)
- Partner across national and state as well as academia and industry for visibility in threat actors (Disrupt)

Prepare for Atrocities Before They Happen

- Build in ability to prepare for and respond to multiple threats at once (e.g. simultaneous health epidemic and widespread riots) (Disrupt/Mitigate)
- Widened testing for/ surveillance of threats within food chains (Disrupt/Mitigate)
- Fund research projects (i.e. securing the home-to-corporate network concept as more people work remotely) (Disrupt)
- Conduct drills for city-wide evacuation and emergency response of WMD and DWMD (Disrupt)
- Preparation & training for emergency services to respond to wide scale cyber attack on critical infrastructure (electrical disruption, IT, analog failsafes, etc) (Disrupt)
- Explore and specify how the Biological Hybrid expands monitoring and partnership requirements (Disrupt/Mitigate)

Design Complex Systems with Security in Mind

- Create laws and policies that address changing norms related to human manipulation via machine (Disrupt)
- Develop standards and guidelines for genomic data collection, storage, resale, and commercialization (Disrupt)
- Enable redundant and backup response and recovery capabilities in emergency management programs (Mitigate)
- Secure supply chains of vaccine and crisis response materials (Disrupt)
- Establish trusted, authoritative sources of information during all stages of attack (Disrupt/Mitigate/Recovery)
- Develop policies to monitor domestic cyber infrastructure, data sharing, and accountability for mitigation and recovery of infrastructure compromise (Disrupt/Mitigate)
- Explore how the Cyber Aided WMD Framework changes responses to a cyber enabled WMD (Disrupt/Mitigate/Recover)

Strategic Mindset Shifts

- Research the implication of a shift from Destruction to Destabilization (policy, budget, legal, etc.) (Disrupt)
- Research and pilot methods to improve ability to attribute cyber attacks (Disrupt)
- Research protocols and industry standards to secure the home-to-corporate network concept as more people work remotely (Mitigate)
- Begin explorations and set research agendas around DWMD and Cyber Aided WMD framework (Disrupt/Mitigate/Recovery)

Know thy enemy

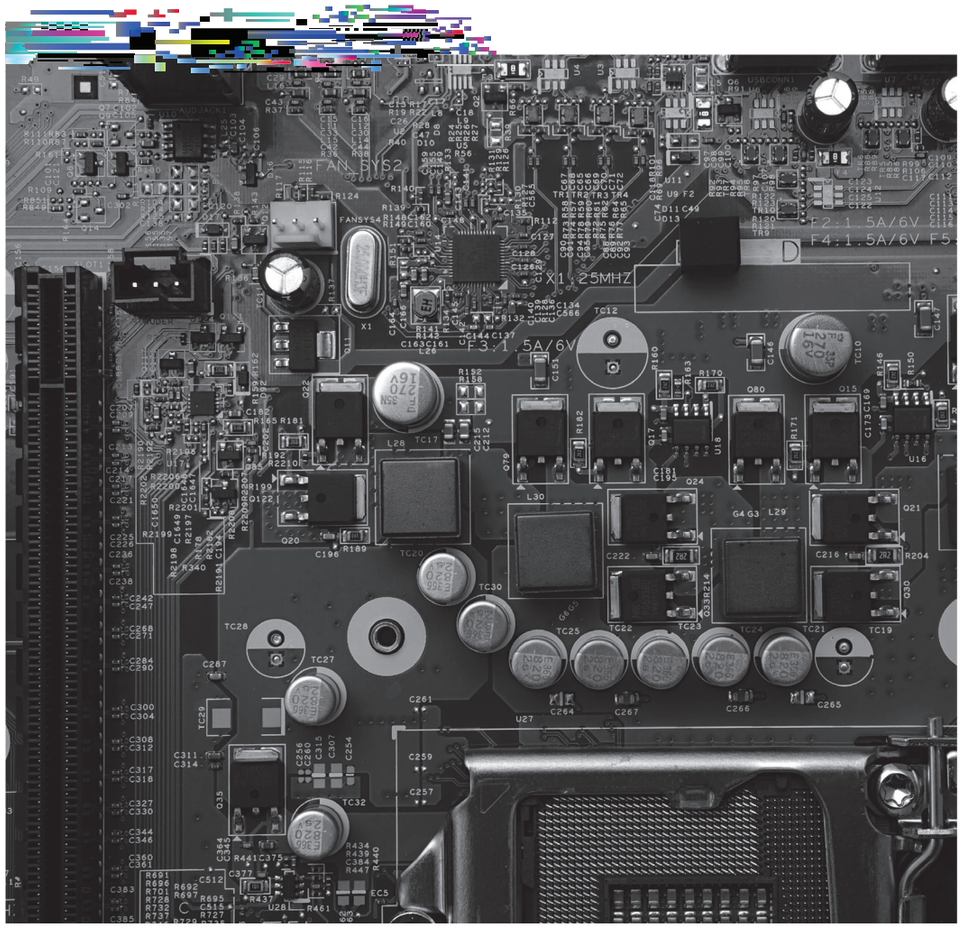
- Research and explore the role of dark web marketplaces for cyber aided WMD effects (Disrupt/Mitigate)
- Work to become trusted, authoritative sources of information (Disrupt/Mitigate)
- Advise government on emerging technology novelties that would exacerbate disruption (e.g. social media trolls, mis-information bots, censorship tools, etc) (Disrupt)
- Explore weak points and opportunities in the Cyber Aided WMD Framework for adversarial exploitation (Disrupt/Mitigate)

Prepare for Atrocities Before They Happen

- Simulate scenarios of 2nd & 3rd order mass atrocities after WMD event (Disrupt)
- Understand and advise on the effects of increasing automated agriculture and food production (Disrupt/Mitigate)
- Develop better education and research showing how and under what circumstances people might fall victim to mis- and dis-information (Disrupt)
- Research the possible effects of The Biological Hybrid (Disrupt)

Design Complex Systems with Security in Mind

- Research what changes need to happen in engineering education to prioritize security in complex system design (Disrupt)
- Pilot research and create medical devices with security-by-design principles (Disrupt)
- Develop new approaches for building expert and community confidence in safety and security (without further compromising systems for adversaries) (Disrupt)



Strategic Mindset Shifts

- Explore the implication and business impact for a shift from Destruction to Destabilization (partnerships, liability, designation of private sector assets as critical infrastructure [physical and digital]) (Disrupt)
- Examine across markets how to improve methods of communication and sharing to increase the ability to attribute cyber attacks at mass scale (Disrupt)
- Begin public conversation about DWMD and Cyber aided WMD (Disrupt/Mitigate/Recovery)
- Understand and communicate roles and stakeholders for a cyber aided WMD attack (Disrupt/Mitigate/Recovery)
- Research protocols and industry standards to secure the home-to-corporate network concept as more people work remotely (Mitigate)

Know thy enemy

- Develop processes and procedures to detect and guard against a dark web marketplace for cyber aided WMD effects (Disrupt/Mitigate)
- Develop sharing networks to bring together industry as trusted, authoritative sources of information (Disrupt/Mitigate)
- Advise government on emerging technology novelties that would exacerbate disruption (e.g. social media trolls, mis-information bots, censorship tools, etc) (Disrupt/Mitigate)

Prepare for Atrocities Before They Happen

- Simulate scenarios of 2nd & 3rd order mass atrocities after WMD event (Disrupt)
- Understand and advise on the effects of increasing automated industries (e.g. agriculture, food production, supply chain, transportation, etc.) (Disrupt/Mitigate)
- Review current product and markets to understand how and under what circumstances people might fall victim to mis- and dis-information (Disrupt)
- Practice and set processes for industrial critical infrastructure attacks and failures (e.g. financial, energy, IT or information, etc) (Disrupt/Mitigate/Recovery)
- Explore the possible effects of The Biological Hybrid on systems, how to detect it, areas to watch and how to alert the authorities (Disrupt/Mitigation)

Design Complex Systems with Security in Mind

- Explore what changes need to happen in engineering teams and procedures to prioritize security in complex system design (Disrupt)
- Develop new approaches for building expert and community confidence in safety and security (without further compromising systems for adversaries) (Disrupt)
- Explore and set processes for industrial critical infrastructure attacks and failures (e.g. financial, energy, IT or information, etc) (Disrupt/Mitigate/Recovery)
- Explore how the Cyber Aided WMD Framework can be integrated into industry monitoring and response across fundamental stakeholders (Disrupt/Mitigate/Recover)

APPENDIX 1: ACRONYMS

DNA	**Deoxyribonucleic Acid**
DTRA	**Defense Threat Reduction Agency**
DWMD	**Digital Weapons of Mass Destabilization**
GDP	**Gross Domestic Product**
IOT	**Internet of Things**
IT	**Information Technology**
SCADA	**Supervisory Control and Data Acquisition**
WMD	**Weapon(s) of Mass Destruction**

APPENDIX 2: SUBJECT MATTER EXPERT VIDEO TRANSCRIPTS

These transcripts were machine transcribed from video recordings of the subject matter experts who presented expert perspectives at the beginning of the threatcasting workshop. The transcripts have not been further edited for formatting, spelling, or punctuation.

David Aucsmith, Senior Principal Research Scientist, Applied Physics Laboratory, University of Washington, 28 Jan 2020

Okay. So I was looking at this along two vectors. If we want to know what the future will be, it's better to understand how we got here, like the past. So the two vectors, the first is I've been in computer science long enough to where I remember hacking was a good term. It was back when Byte magazine was a big deal, it was a seventies, 80s, et cetera. But I, if we look at what computer attacks looked like from the 80s on, so the first thing that happened was the attacks against the, against the network stacks in the various devices on the internet and this from the Morris worm to the ping of death that Microsoft had. All of those were essentially attacks against how the network stacks behaved and the fact that you could, in the case of the ping of death, you could send a fractured particular type of fractured packet that would cause system shutdown.

Microsoft, Apple and everyone else realized they had to armor the network stacks. And they did that. And those attacks for the most part went away. Then people began to attack the OS's themselves. And that's when Microsoft and Apple and at the time Unix systems, everyone realized that they had to armor the entire OS so we have the Microsoft's great commitment at the time to you know, trustworthy systems and the whole software security, software development, life cycle, etc. So past that point people began to attack the network traffic. And then you had attacks against confidentiality and integrity of the traffic that led to IP sec and other crypto algorithms being used, HTTPs, other things being used to protect that traffic. So if you can sort of see over time, people that simply been moving up stack, if you will, for us software guys. And where what happened in the early two thousands to sort of mid 2000 tens was an attack against the advertised services that were, the devices were actually presenting the OS. I mean, one of them are our network compliance devices. So this was on odd JPEGs or odd video files. And we still see that with Adobe flash and PDFs. To this day because the renderers are being attacked. But we see a lot less of that than we used to. So in essence we figured out how to do that.

So the shift up stack is people began to attack the trust systems underlying those. And I will contend that that's a great deal of where we are now. So phishing is essentially an attack on the internet trust mechanisms where one purports to be from someplace else or or in some way violates your trust in order to get the attack or your assumptions about what's trustworthy uh particularly well known are attacks against X.509 and then some of the inherent protocol problems with that. And now we've gone to a different type of trust mechanism, which is things like deep fakes and, and other things which actually present not attacking the protocols or the infrastructure, but attacking the information itself and, and rendering it susceptible to misunderstanding. And the interesting thing here is if, if your, if your goal is to sow confusion, it turns out to be relatively easy because humans have a very low tolerance for false positives.

So if you, if you can misshape the information in some that you know, it's just traditional information warfare. If you can misshape the information such that humans can understand what to believe in, what's good, what's bad then that becomes a very powerful tool that if you will, that's the technical vector. So let's set that aside and look at a different vector, which is along cyber warfare. And the easiest way to look at cyber warfare right at the moment is this sort of three traditional ways you can do. You can integrate computers in warfare. The first and the simplest is network centric warfare. That's Admiral Cebrowski's work. And that is simply just integrating in computers into the mechanisms of warfare. This is using computer controlled artillery, fire using GPS and satellites to do geolocation integrate that in its information back a battlefield awareness.

It's all of those things. It's what all modern militaries do. Now. It's expensive and it's sort of big military, if you will. The second way I can do is I can actually use pure cyber as an adjunct through traditional military means. The Russians before they went into Georgia are the sort of quintessential example of this where they shut down the communications infrastructure before moving and physical assets, tanks. They blocked the command and control networks. They kept the president from being able to communicate either to the public or his own troops. And that is now sort of doctrine and warfare as we understand it. All militaries practice one level of that. The third, and these are, these are actually in linear, time sequence order as well as in terms of how they were developed.

The third is pure cyber. So cyber on cyber. And here we're really talking cyber physical systems because the only way to have a real effect in the physical world from cyberspace is at the interfaces of the cyber and physical world. Cyber physical systems. I mean, clearly you can erase information and you can sow discord. You can. Sow mistrust, et cetera, as I went through on a talk on injecting into the information itself. But if you actually want to damage things or cause a permanent effect, it has to be cyber physical systems. And the unfortunate thing here is that most systems are now cyber physical systems migrated such that that's the norm rather than the exception. So SCADA systems for example. And we have seen a rising increase in attack on cyber physical systems.

I do, I lecture in the military. And one of the things I point out for the Navy is a warship is simply a floating SCADA system. And if I want to disable a warship, I don't have anywhere near it as long as I can communicate to it. And most cyber physical systems hadn't, cyber physical is somewhere where the operating systems were in the early 1990s, where they were essentially designed against failure and against you know, sort of mishandling and, and user error and all the other things we do when we built software systems. They were not designed for an adversarial environment, by and large. We're going to have this to continue and there's, there's going to be, you know, significant problems brought about because of that, and if I sorta, let's combine the two factors if you will. So we've got the misinformation and the ability to influence the information itself and we have cyber-physical systems.

So the best why my, I have a deep worry about autonomously driving automobiles, for

example, because a great deal of research has gone into those. And, and this is not just the commercial sector, the military sector as well with its role on battlefield robotics. For the most part, those have been designed without seriously considering the actions of an adversary against them and an adversary that is consciously trying to affect their behavior. There's some excellent work that was done by simply putting interesting markings on a stop sign, which led a number of the self-driving auto algorithms to recognize that as a sign of some other type. For example, a 45 mile per hour speed limit sign in one case. So one of the problems with machine learning and deep learning and those types of algorithms is they really can't tell you if you will know how they arrived at that conclusion. And so backing out what was done to affect them is actually very difficult. So we bring all that together. What I think in terms of mass problems would be some sort of attack that injects unknowns or or non-trust into cyber physical systems that we need an app to operate. Whether that's a power system, the electrical grid or other things. And that sort of, if you will, the cyber equivalent or WMD in the longterm. Oddly enough, there's at least for part of it, there is actually a pretty good fix. But again, I go back to where computer systems were, for example, Microsoft where I spent time in the, in the 90s. We don't have the right engineering mechanisms in place to help mitigate that. An example, contrary to Hollywood, it's impossible to have green lights at 90 degree angles on a traffic light. You can't do that because the people who build traffic lights are smarter than that. They weren't worried about cyber attacks, they're worried about a failure mode. So if the light failed with not with greens at 90 degree angles and people smashed into each other and people died, the traffic light company would be sued out of existence.

So they designed the systems and if we go back to the relay days before it was all computer control, it was essentially a bar inside of the traffic light and it moved up and down connecting, you know, a big relay and the traffic light was only capable of moving from one safe state to another safe state. Now you might be able to keep it from moving so that only one direction of traffic gets to go the entire time. And that would indeed cause chaos. But it's not the same as affecting the traffic lights so that people crash into each other. Another example is from the aircraft industry are the flaps on aircraft. The requirement is that they'd be physically connected because there is not a safe state of asymmetric flaps, period. That just doesn't exist. Therefore, the flaps have to be linked so that they can never be asymmetric.

What this gets into is essentially people will build cyber physical systems forget that there's a physical component to them and now we make them essentially small computers that can do, like our general purpose, computers on our desktop can do anything. They shouldn't be able to do anything because they're not a computer. They're a specific functioning device. And we need to think about that in terms of the mechanical aspects of physical aspects so that we limit what the computer can do. There's a notion of computer scientists that all computers should be capable of doing anything and they're infinitely adaptable. That's actually not the best solution for a lot of problems. It turns out. So those are, if you will, sort of the two places that I think this is going. And then if you lay on top of this, of course the continued interaction and how many people are connected and the speed of the connections and the ability to respond to changes in the system.

Any flaws like this that can be amplified on a mass scale become something equivalent to a weapon of mass destruction. And I think it's a problem that many people have when they think the computer is not in terms of mass destruction. But when we get to a cyber physical systems, we are talking about mass destruction. So anyway, that's my thoughts. So, that's my talk.

Name withheld, 31 Jan 2020

My name is (omitted). I'm a professor of history at (omitted) where I also direct the (omitted). And what I'm going to do today is talk to you about my thoughts on cyber, what WMDs and mass atrocities. And first I'll start by telling you what mass atrocities actually are. In the past, we've, people in my field have focused on genocide prevention, but what we now do, especially because in the policy community community, it's much more palatable, is to use the concept of mass atrocities. And that is not something formal. There is no legal definition, but it includes genocide, war crimes, crimes against humanity and ethnic cleansing. And it normally means that there must be a large scale systematic attack or violence against civilian populations.

The major question in our field is what shifts a country or a region from being at risk to actually having a mass atrocity? And the short answer is we don't always know. In fact, we're not very good at predicting these things. However, we do know that conflict, especially those involving WMDs and in the future, particularly cyber weapons and information warfare will play an outsized role. And in fact, if a WMD is used, I would make the suggestion that in addition to being a mass atrocity itself, it is likely to trigger follow on mass atrocities and that's something important to consider.

I'm going to give you six main considerations of how mass atrocity relates to thinking about threats of future use of WMDs or cyber WMDs. First and most important is that mass atrocities are processes. They're not events, they don't occur out of nowhere but they often surprise us because we do not like to think about preventative measures. And this thinking is unlikely to change in the future.

Second, future use of a WMD might not be the biggest disaster. The follow on mass atrocity might. If we consider the Rwandan genocide akin to a WMD attack resulting in the deaths of about 800,000 Tutsi and Hutu in about a hundred days. That disaster in and of itself, that catastrophe is one of epic proportions. However, it pales in comparison to the violence. It spurred in the Democratic Republic of the Congo where since 1995 over 5 million people have died, hundreds of thousands remain displaced, militias and Ebola thrive, and centralized governance fails. As we think about future threats, we have to think about the second and third order effects of the use of a WMD, not just the first order.

This leads to point three which is that mass atrocities occur when conflict occurs and atrocity producing conflicts are on the rise. 85% of atrocities since 1900 had occurred during an ongoing conflict and civil war is increasing, not decreasing in our current society. The incidence of civil wars has increased tenfold since the end of the cold war when compared to the period covering 1820 to 1989. Civil war now last as much as four times longer than interstate Wars. These civil Wars are now on average, three times more deadly than they were in the first half of the 20th century, and instances of ethnic cleansing, another atrocity crime, these instances are increasing, not decreasing. The Freedom in the World report lists 11 cases in 2008 excuse me, 2019 compared to three in 2005 and the likelihood of conflict will continue to increase exacerbated by many factors that I'm sure

others have spoken to you about. But these include global wealth inequalities and climate change. The Department of Defense has estimated that climate change will decrease global GDP by about 10% by 2100 and there are certain the more conflicts and more violence tied to climate like that in the Sahel which has produced great great potential to result in mass atrocities like those perpetrated by Boko Haram in Nigeria and the Janjaweed in Darfour, Sudan.

Conflicts themselves are becoming more complex. As of 2019, the average civil war now has 14 different parties involved including proxy States, non state actors, regional state actors where central States fail and civilians are increasingly becoming targets. Urban warfare is on the rise and when attacks occur in cities, 92% of the casualties are civilians. Complex conflicts are generating more refugees and asylum seekers and internally displaced people than at any time since world war II. In Bangladesh alone, there are more than 800,000 Rohingya, perhaps about a million Rohingya in one massive refugee camp in Cox's Bazar.

Now to my fourth point. Information is the real cyber weapon of mass destruction and cyber WMDs are already being deployed, exacerbating conflict risk and risk to civilians. While other experts you hear may differ, I would argue that the world is currently still absorbing a bomb blast or the bomb blast of an incredibly effective cyber attack. Russian interference in the last and the last U S election and ongoing Russian exploitation of political division within the U.S. and elsewhere around the globe. The internet has made the speed of information delivery virtually instantaneous and this is destabilized concepts of truth, sensational or false news is six times more likely to be read than truthful news and 30 times more likely to be forwarded. This can exacerbate existing fears and societal tensions and divisions at incredible speeds. An example of this is the violence in Myanmar in 2014 and 2017 which was fed by calls to kill Rohingya circulated through Facebook. This provocation of partisanism divisiveness, compassion fade, and attacks on truth are now easier and quicker than ever. This global information crisis is likely to worsen, not improve as more States weaponize information in the cyber realm, sowing fear, doubt and chaos. This chaos will be increasingly difficult to manage as the power of policymakers to tamp down on it wanes and the advantages of exploiting it grow.

Point five. We tend to misunderstand the reasons for perpetration and this knowledge that we draw from atrocity prevention scholars will be helpful for us to better understand the risk of of, excuse me, of mass atrocities through weapons of mass destruction in the future. We find it difficult to emphasize with our adversaries and that is the cause of part of our misunderstanding. People who perpetrate mass violence generally do not think of themselves as bad people. In fact, many of them felt many think of themselves as doing good. There are ideological killers, people who believe in the righteousness of their project that are so it's popularity, the idea of self defense, the idea that there is a cause that they are following. There are of course bigoted killers who have prejudice. There are those who are violent killers, people who kill because of the joy of being involved in violence. And one of the things we are learning is that women kill as well. And this is increasingly a phenomenon in certain areas. However, we should not overestimate the number of perpetrators drawn to killing for ideological, political or religious reasons. We tend to like mono-causal explanations and we have to actively resist them and the pressure from our leaders and information consumers to have them.

We should resist using concepts of good and bad. They don't work. Many people kill because they fear if they don't, they themselves will be killed. There are careerist killers who comply for career prospects or gain by their involvement. There are materialists killers, people who get direct economic advantage, either jobs, property or businesses from involvement in killing or are mercenaries. And we are seeing an increase in the role that mercenaries are playing worldwide. There are disciplined killers, those who are involved in organizations and value obedience and conformity, comradely killers who kill because of peer pressure or fear of being left out. Bureaucratic killers: Those who just enable the processes that allow people to be killed and this understanding of the multi causal reasons for perpetration is important as we think about the possible future uses of weapons of mass destruction.

And finally, sixth. We underestimate the negatives of nation state thinking. While the concept of the nation can be inclusive, it is more often used to exclude and divide, to restrict rights, privileges and wealth, and to stymie the growth of international institutions, at least within the last 10 to 15 years. We're experiencing a global swing where democracies are being eroded. One party and authoritarian rule is on the rise and legal protections are also on the decline. We're seeing the dismantling not the construction of international organizations, and this is produced what David Miliband, the head of the International Rescue Committee has called the "era of impunity" in which concepts we once thought were universal and inexorable, such as protection of human rights, the rule of law, accountability for crimes, all of these have diminished.

So quick conclusions: as we consider future threats, we should remember one, mass atrocities are likely to be part of the equation. Two, the occurrence of a mass atrocity will likely mean that the second order effects are more destructive than the first. Three, information may be the greatest cyber weapon. Four, we need to understand the nuanced reasons for perpetration, i.e., that there may be many motives for the use of cyber weapons or cyber WMDs. And fifth, the root cause of why people may use cyber weapons and other WMDs as likely to be justified as a moral good, perhaps based on nationalism.

Dean Hachamovitch, 31 Jan 2020

I'll just, I'll just start in from, from our conversation. I think a good place to start is that industry is actually pretty good for the attacks they are aware of and are concerned about. And you know, you and I talked about FinTech and this notion of fraud. They understand that there's fraud if they can limit fraud to a certain window, that's fine. So again, like the industry is, is more than competent at what it's good at. Of course, the caveat here is, you know, I've got a sprinkle of headlines around Google getting fined and Facebook getting fined and these are some of the best practitioners in the world. So even the best has got

some limits. I think the biggest challenge is there is a completely different set of attacks because there's a completely different set of goals. So typically, you know, there's a really straight forward attack. Like I want to when I can own your box and I can compromise that, I can do all sorts of interesting things.

That's nice. It's also kind of hard in some circumstances. And there are all these other examples and maybe I should start with examples and then abstract upsets. In philosophy. Long time ago, a company that makes a desktop operating system started running the service that all the PCs in the world could connect to and automatically get updates and stuff. And in a meeting somebody asked, has anyone thought about what happens if a bunch of folks with weapons show up at the door and a USB stick and say, we have something, please deliver right now to everyone.

That's a great example of we're really used to, Oh wow, what if there's, you know, cross site scripting. What if there is, you know, an escape from the sandbox. We didn't really think about, you know, the equivalent of box cutters, you know, and just like, no, we're going to deliver this stuff right through the front door. Just not something was really on our radar when we looked at a threat model at all. Maybe that's the, that's the, that's a good phrase. The need to completely rethink what a threat model looks like and how many how many of the foods touch, how many different pieces of tech touch each other. Now, another example that came up in conversation not long ago you know these groups that are doing the various things need funding. Here's an easy way to get funding. I'm not recommending this. This is all in scare quotes.

Go and do a completely legal take, a very legal and short position on some tech stocks. Make every smart speaker in the home suddenly start speaking in gibberish all at the same time because how good is the security? It's, it's not even all of them; if you can get a bunch of them? Wow. There are headlines and people are concerned and people lack trust and everything goes down and you cash in your shorts and you've got a lot of funding to keep going. You've also shattered confidence in a system and there aren't that many industrial attacks that are, "I want to take you out by shattering confidence in who you are and what you do." Classically, I think industrial attacks had been much narrower or had different goals. This is one where, we're, you know, you can imagine if it, I'll just go back to the speaker when instead of making another one, if, if all, if everyone's tech started sailing in a particular way, even if the quote "literal damage" was pretty minimal, the larger psychic challenge, and this might be the difference between weapons of mass destruction, mass destruction and weapons of mass terror comes into play -- I don't want to get semantic about it. I'll pause there, 'cause I think it's a healthy spot around industry and goals and TMAs.

Yeah. And, and you had mentioned that, you know, if we're going to have a digital weapon of mass destruction, then it will and probably will not start in infrastructure, will not sit there till actually start in the private sector.

Yeah. And look, no one ever puffs their chest out and says, my industry is amazing. Our stuff is unbreakable. I mean, what kind of company would go and make that kind of a claim? The thing about infrastructure is we're all kind of aware of infrastructure and our scare. And so infrastructure gets some interesting attention. Even though I think it's like squirrels or chipmunks are the leading source of power outages, trust me, someone can eclipse them pretty soon if they really tried. The problem is the folks who don't realize they're part of the attack surface or that they're part of the chain of the attack surface. So the Windows update example I gave you know, is one. There are all sorts of other pieces of tech that that aren't even the, I'm sorry, I should go back. I'll just focus on the private sector, laundry services and linen services.

If you compromised a laundry or linen service that served, that helped food establishments for hospitals, there's a tremendous amount of damage you could do, just there. And so I think one of our challenges is we think about infrastructure very differently than we think about private sector goods that are transacted. And the set of the way we think about infrastructure is different. We don't realize that at some point everything is infrastructure because at some point the platform became everything. Like the webs of platform. And my Iphone's a platform. And anything that can run some code is a platform. My Ring doorbell is a platform. It looks as if all the Ring doorbells in the world suddenly started speaking in tongues. Wow. That would be shattering. And again, like is that infrastructure? Yeah, it's public infrastructure. Look at how law enforcement is using it.

And so you had mentioned in our previous conversation as you start to look at weapons of mass destruction, specifically digital weapons of mass destruction, it's the M that really matters, especially when you're talking about industry. Could you talk a little bit about the verticals, like thinking about what is the vertical or where could the attack be where you get the maximum amount of M?

Yeah. And so, so I think that it used to be, before we were this connected, that you would just choose one thing and you would attack it and it would be great. And I'm not sure what the threshold for M in WMD is. What I know is that you can essentially have one system tip over and another tip over another, and ironically we'd call that chain reaction. So you know, for example, if if an attacker simply delayed all SMS messages, some large fraction of SMS messages foiling a whole lot of two factor auth. Wow. There is a telecom hiccup that really messes up finance. Now let's say they targeted finance that worked in some particular group. Wow. Now it's finance tipping over something else. You could imagine that, you know, pretty much everyone relies on finance and thus everyone relies on telecommunications. And so we have a, we have a stack where not everything that can be attacked and essentially chain into another problem, it's not necessarily defended that way.

Andrew Hessel, 17 Dec 2019

Great. I'll just start by introducing myself - my name is Andrew Hessel. I am the President of a seed-stage company called Humane Genomics that does synthetic virus engineering. I'm also the co-founder and co-executive director of the Genome Project Write, which is essentially the successor to the Human Genome Project. Instead of reading large genomes

we're learning how to write them.

I basically think about biology all the time and not just kind of the low-level mechanics of biology which is all based on the cell, but on how biology is becoming programmable. For almost 20 years now I've been interested in the technology that's become known as synthetic biology, which is really the next generation of genetic engineering. It's supported by digital tools and technologies: essentially CAD software for living things; large data sets that have come out of the scientific world over the last 30 or 40 years, including large DNA sequence databases; and ultimately lab automation that essentially reduces or eliminates the needs for bench laboratories.

So, combined, these technologies make it much easier to design and build biological systems. And I'm particularly interested in the design, and construction, and boot-up of complete genomes: plant, animal, bacterial, or viral.

Because it's still early days in this field the genomes that have been made for pretty much the last 20 years tend to be small genomes. Right now about 35 virus genomes have been constructed from scratch, three bacterial genomes, and we're just doing the finishing work on the first eukaryotic genome, which is yeast. And that's pretty much where the field is, but it's becoming pretty straightforward now to start building viruses.

The tools and technologies for doing that are sufficiently accessible, inexpensive, and robust that today, to build a small synthetic virus -- a small genomed synthetic virus -- is on the order of a few weeks for a few thousand dollars.

I think this is really important when it comes to understanding some of the biological threats in the world, because people tend to worry about some of the biosecurity issues, but we don't generally worry about plants taking over the world. We have plenty of antibiotics. Large organisms aren't generally a threat to humanity anymore, but the virus continues to be a scourge every year. And it's seasonal flu sometimes, so, you know, it's a good reminder.

In general, we have very few viral defenses that are effective. My son had the flu a couple of weeks ago; took him in to the doctor. There was no rapid diagnostic test used to even identify that he had the flu, of what variant of flu it was -- was it a more serious one, etc. There's no real medications that can be given, except in the very early stages of the infection where Tamilflu can be effective.

So, we're pretty much blind and incapable of doing any type of remediation for infectious viral diseases at this point. In a world where just about anyone with a few resources and some will can build a virus, I think that's no longer acceptable.

To give you some examples of just how bad this could be, there's only one virus infection that that kind of stands out in the last 100 years and it's the 1918 influenza, so essentially flu season 1918. It supposedly killed between fifty and one hundred million people; the records weren't well kept back then, but that's at least double the deaths of the first World War. And that's just remarkable.

Granted, our options for treating flu at the time were limited, even recognizing [inaudible]. We didn't even have antibiotics. But today, if a similar flu was spread around the world and caused a similar number of casualties, it would equate to about four hundred million people.

And really, we don't have many other pharmaceutical approaches for treating them. Even then a fast-acting, highly infectious and potentially deadly virus would be identified quite early and humanity would change their behavior very quickly.

But slow viruses exist -- viruses that have extremely long latency periods, sometimes on the order of years. That to me is one of the reasons I think we need to completely revamp our viral defense system right now, since if one of those agents were spreading today in the world we wouldn't catch it.

And just imagine if dementia was weaponized as an infectious disease.

Michael J. Hopmeier, President, Unconventional Concepts, Inc., 27 Dec 2019

Great! So, hello everyone, my name is Mike Hopmeier. I've been asked to chat for a few minutes on different ways of looking at methods to screw up the world. When I look at a lot of these challenges, whether it's traditional conventional role of weapons of mass destruction or doing evolving challenges with the information and the internet, I really look at end effects, not causes.

We've traditionally looked at the fact that, whether I'm talking about chem, bio, or nuke, improvised explosive devices and such, we talk in terms of physical destruction or mortality and morbidity, and I think that's too narrow a view.

As we've seen society evolve, it is not that a lot of these different weapons and capabilities become more powerful and capable, it's that in a lot of ways, we've made ourselves more vulnerable.

For example, if we take a look at bio effects, just consider that even 15-20 years ago the principal threats that we were dealing with were a small number of people, individuals, and massive infrastructure to support them, such as biopreparat in the former Soviet Union, and the potential threat damage they could do.

But if you take a look at simply the number of fatalities associated with bio-attacks from the Soviet Union and compare that to the number of fatalities and impact, say, anti-vaccers have had, through the effect of measles and fatalities we've had all over the world, and societal impact - it's been much greater.

I think that we really need to broaden out our point of view when we look at WMD, to think about these broader effects: the ability to either be opportunistic, for example. If you take a look at the last 50 years in the bio arena you can find out that on average about every thirteen months there's been a new or unusually emerging disease that's come out.

Whether we look at Zica, or SARS, or various hemorrhagic fevers, somebody through use of the internet and collection of data, and a little bit of forward planning, can go ahead and take advantage of these opportunistically to scare and have a big effect on society.

When we look at cyber in particular, it's traditionally been a contact sport, if you will, where if we wanted to recruit an extremist, we had to identify them, be able to talk with them, get an understanding of what their real interests are, how they view the world, get to know them and convince them to engage or become a fanatic.

Today, with access to large databases of information, marketing for example, if we look at all the information that's collected in the Googles and Facebooks and such, being able to not only identify those individuals and personalities that are particularly vulnerable and susceptible to recruitment and being swayed to be an extremist.

But when you combine that with new methods of artificial intelligence, machine learning, and various automation techniques that are available and out there, it no longer becomes a one-on-one issue. I no longer have to identify particular individuals; I can identify them in groups, wholesale, and recruit them and have the ability to point them in a general direction to cause significant impact.

If we think back, oh, it must be 30-40 years now, Larry Niven had developed the concept and first written up the idea of a flash mob, where people go on teleportation discs and all of a sudden appear at a given point and cause all sorts of chaos. Today, if we look at the ability of broad-based communication to a wide array of people -- Twitter and Facebook and these other groups -- we already see cases where we have flash mobs occurring today with modern use of communications and cyber. And for the most part, they are innocuous. They show up and suddenly pull out their violins and play classical music in a train station, for example.

But what are the other potential things that we can see that go well beyond, such as the Arab Spring?

The point is, that simply looking at the technologies themselves, the direct impact, whether it is biological warfare, or DIY bio as it's evolving into, or use of nuclear/chemical weapons, or even improvised explosive devices. Most of our threat assessment and analysis is still focused on what is the threat that we are actually trying to create? What is the damage? When in fact we really need to start, I think, broadening our points of view and perception and looking at the impact the different techniques and methods have.

While it's great to look at things like Richard Danzig's concept of "reload" -- how rapidly can you manufacture large quantities of weapon-grade Anthrax and employ it over a number of cities -- the fact is I can create as much or more societal impact if I simply get the world to believe that there are two or three cases of smallpox out in the wild running around.

Now, that may be based on the fact that there is real smallpox, but even if there isn't, even if there are diseases similar, any case of smallpox or something similar occurring anywhere in the wild, that is confirmed or appears to be confirmed, anywhere in the world, we're immediately going to our maximum level of response; there is no intermediate level.

So the idea really is, and I think the challenge is, to look at the effect and how cyber and information is going to affect society. The bottom line is, if a threat is not going to impact society, if we're not going to change our way of life, if there aren't going to be a huge number of people dying that try and change our way of life, if we're not going to be able to significantly damage or alter our infrastructure, it probably really doesn't matter.

And I think that's the real challenge we have, is looking at effects, rather than causes. Thank you!

Name withheld, 22 Jan 2020

Okay. I'm (omitted) and I'm going to talk a little bit about the intersection between cybersecurity and cyber risk and also risks around WMDs in particular as they relate to synthetic biology and what, what we call genomic security. And so thinking about 10 years out in the threat landscape, I think there's a few issues I'll, I want to talk about that I think really everyone should be considering in this space. The first is, is around specifically synthetic biology. Increased automation miniaturization and democratization have changed synthetic biology. This trend is directly leading to systems that produce biological material, either organismal or nucleic acids. And as these systems become increasingly computational, there's an increased risk of, of cyber threats. This includes not only industrial production, but also critical systems producing medical countermeasures. So systems that absolutely have to be used absolutely have to be available at the time that we need them.

The second issue is an attack on critical infrastructure and an erosion of trust and core capabilities does not require high mortality or morbidity events. Efforts by hackers and trolls to sow discord and promote disinformation may have similar impacts as biological WMDs, especially if paired with an accidental or naturally occurring event or disaster. The kinds of things we see routinely happen but, but don't pay critical attention to them. The third issue is we do not yet know or understand the full implications from a WMD perspective of a large portion of the population having their full genome sequences available. And these data potentially are being left unsecured and at a risk of collection or harvesting by, by motivated threat actors or hackers. The fourth issue is the current state of venture capital. Funding in, in biology is heavily driven by quick to market motivations.

This is led security, especially cybersecurity to take a back seat and be viewed, be viewed essentially as a cost center rather than a critical component to public safety. This means that really advanced and biology with potentially high dual use capabilities are being developed and developed without adequate safeguards to prevent potentially unattributable use by hackers and adversaries. The fifth thing is the lessons of cybersecurity in the internet were hard won and took over a decade to be understood. And we're still wrestling with the implications of transitioning from an open academic system to a closed system with high levels of potential risks. As synthetic biology matures from

an academic pursuit to a commercial enterprise, it's essential that we learn these lessons quicker and work faster to bake cybersecurity and from the beginning before hackers and adversaries fully appreciate that synthetic biology as a means of taking raw information, raw computational information, and deploying it in organisms that can grow and in fact, and move with without subsequent intervention.

The Impact of Computing and AI on the Threat of Biological Weapons in the Coming Decades

B.K., 31 Jan 2020

As we progress into 2020, the impact of computing on biological engineering is utterly apparent and at the same time, not necessarily what was expected.

My unique contribution to this discussion is an acute awareness of biological weapons. The development of biological weapons is indeed a kind of biological engineering, similar to innovating agricultural products, food products, medical biologics, and so on – especially in the case of new toxins. Innovation of infectious agents is particular and unique; because the natural agents are in many ways already optimized for many of the same properties which are desired in the weapon. These include virulence and transmissibility.

Reflecting on this, the earliest biological weapons – still used today – were famously simply dead bodies; used to spoil wells or thrown into crowded fortresses during sieges. The use of dead bodies to spread infectious disease was crude but not silly and grew directly from the observation of infectious disease, itself a major intellectual step forward in both curing and causing disease. It had some key limitations – it wasn't always clear which diseases could be transmitted in that fashion, and additionally, to acquire a freshly deceased patient usually required the disease to be circulating among one's own forces or camp followers. In this sense, biological weapons were largely only available to those already suffering their effects.

Biological weapons advanced considerably with the ability to isolate, identify, cultivate, and preserve specific microorganisms. In a sense, this moved the practice from 'hunter-gatherer' to agricultural.' This set of capabilities drove all the innovations of the World Wars and frankly, the Cold War. When the United States and Soviet Union dismantled their biological weapons programs, they were industrial era programs using industrial agricultural or food-processing techniques, which were also used in the pharmaceutical industry. For the most part; however, biology was militarily intractable. The weapons were crude, impractical and found very little use. There is no doubt that had the Soviet Union reversed the outcome in Afghanistan with any of the biological weapons in its vast arsenal, it would have done so. That it did not does not call out restraint, but rather inability.

For decades, a revolution in biology was sought in mathematics. There were repeated attempts to introduce modern mathematics into the heart of biology throughout the 20th century – with some peripheral successes but overall, derided as 'physics envy.' Feynman himself said the essence of biology was not theoretical, but instead observational: "look at the thing." It was somehow inferred as a flaw in biology that the field did not suit itself to small systems of ordinary differential equations and simple geometries. Actually, many fields did not, and some – like economics and sociology – were greatly distorted by that Procrustean bed. Biology resisted simplistic analysis, even when that analysis was called 'complexity theory,' and biological engineering has proven largely impenetrable to formal methods. This led to decades of disappointment for those who expected rational design of biologics, rational genetic engineering, genome medicine, and so on to revolutionize these fields.

A touch of humor, then, finds mathematics itself turned upside down by computation and the acceptance of computability as an underlying structural element in pure mathematics. Quantum computing will propagate another shock through mathematics, making it more observational and experimental in practice, as it plumbs the depths of reality. Meanwhile, statistics are also in the process of a complete revolution, sometimes misunderstood as the rise of Bayesian thinking, but really driven by computability replacing the logical structure imposed by proofs and embodied practically in rules of thumb, simple tests, and look-up tables.

Biology is similarly undergoing a revolution: sometimes reflected in data types and volumes, but really characterized by the need to shift high dimensional probability distributions, generate population level estimates from individual-level measurements, and effectively connect features across scales spanning many orders of magnitude without resorting to crude measures of center/variance. In the laboratory, the core of this revolution is incarnate in high-content screening, but also various other kinds of highly parallel and sometimes spatially explicit data collection strategies, taking many kinds of measurements of numerous individual entities. The ability to screen libraries of 1012-15 molecules or cells, to monitor the range of diversity within a tumor at the single cell level, to track the life history and migration of every single bird (or bacteria) in a population – this revolutionizes biological engineering.

How does it do so? In part, it frees the biologist from the internal (population-level) conflicts that have undermined in vitro evolution as an engineering method in the past. Now the scientist can expect to track every mutation – and every combination of mutations – and soon the spatial aggregates of diverse co-adapted complexes of mutations. It also opens up what has been called 'precision medicine.' The death of genomic medicine was not graceful: it was stillborn because of the underlying assumption that human genomic variation in the context of disease was relatively simple. Certainly, the genome of a single human could be summarized by the genome in the germline? Instead, the diversity of genomes within the somatic cells is dramatic, and even whole-human population genome-wide association studies may not be sufficient to disentangle the highly polygenic traits which appear typical. In a fit of pique or despair, the 'omnigenic model' has found traction in genomic medicine.

While glass blowing was a core skill for many young biologists in the mid-20th century, coding is high on the list of required skills in biology now. Even simple operations are

frequently performed at a scale that demands automation, with a degree of insight previously unimagined. This is appropriate to the diversity, complexity, and causal density of biology. While 'big data' in biology has for some time meant citizen science or opportunistic data collection, it can also mean automated laboratories at scales order of magnitude beyond what was prevalent in 2015. Some of the first examples emerged with the 'automated graduate student' performing two-hybrid crosses in yeast to test hypotheses themselves generated computationally, but now methods can insert genes combinatorially into every position in cells, conduct saturation mutagenesis for 3D genome trans-interaction screens, or track every single developing cell in the nervous system of populations of animals across generations.

Tied to selection mechanisms, powerful engineering capabilities can produce biological products which are themselves complex at higher organizational levels and not necessarily amenable to retrospective reductionist analysis; at least, not with full intellectual honesty. A just-so story can always be constructed, but what explanatory power will it hold? In the end, the agricultural technologies resulted in medical and military products which were not fully understood – biologists are yet to plumb the mystery of vaccinia – and these new technologies will enable even more complex feats of engineering.

What does this advance in computation mean for biological warfare? In so much as some threat actors are constrained to use industrial era technologies, it suggests that they will continue to arrive at the same capabilities which have been prevalent for decades. Those who use the medieval methods can still inconvenience people by contaminating food and water, for example. However, public health systems - when functional – are fully capable of containing and managing the resulting outbreaks. Agricultural technologies such as large scale fermentation already enable strategic scales of attack that could simply overwhelm public health, but only at high cost and with ample opportunity for attribution and deterrence.

In so much as national will and senior leader intention exists for biological weapon development and utilization, the introduction of a new paradigm in biology presents a substantial challenge for threat-casting, since the new discovery models have the capability to enhance detection and neutralization technologies at least as much as they do offensive technologies. The engineering of probiotics, functional materials, and other biotechnologies that counter potential weapons may develop more rapidly than the weapons themselves. Without spending too much additional time, it may be helpful to perform a kind of difference-in-differences analysis and tease out three ways that computationally enabled biological engineering can change the relative scale and pace of defensive and offensive biological engineering.

First, if the ideal weapons are closely linked to naturally occurring pathogens in origin and properties – because the pathogens had already developed and subsequently optimized most of the key traits required for pathogenicity – such that the military application primarily involved dispersal in place of natural migration, then biological engineering will have relatively little to contribute to offensive development and the impact of advancements in biological technologies will not be able to greatly enhance the already substantial natural infectious disease threat. Under this model, as a threat to public safety, the agents will tend to be countered by long habits of hygiene, public awareness, and established medical science. Military protective equipment will primarily serve to dampen dispersal and exposure on relatively short time scales at or near the sites of intentional release. Meanwhile, the development of novel counter-measures of a biological nature will have more roof for acceleration by advancements in biological technology. These applications of new technology to new problems will be pushed by high demand from the health care sectors, especially ad demographic factors shift, and require new kinds of public health measures simply to manage endemic disease. That is, the arms race is not only between offensive and defensive biological weapons, but also includes naturally occurring pathogens and the perceptions of them. Offensive technology starts with a formidable lead but has little to gain; meanwhile, the pace of public health will advance drive defense at a pace offense cannot hope to rival.

Second, the size and structure of the technical offensive and defensive communities develop differently in response to computational technology, AI, and information technology, because they are constrained on one hand by security concerns and on the other by the demands of the marketplace. Openness of communication is as important a resource for modern biotechnology as human capital, facilities, or finances. On the offensive side, legal pressures, ethical disapproval, and the requirements of strategic surprise limit collaboration and communication. On the defensive side, intellectual property and export control also limit communication. These limits can lead to fractured communities. Even though fractures disrupt rapid technological progress to a single goal, having many minimally coordinated elements can also lead to a diversity of solutions coexisting as different groups and organizations meet the same offensive or defensive requirements different ways.

Third, while ethical considerations have long tied the hands of defensive scientists operating in public view but less so offensive scientists operating in secrecy, new technologies generally favor experiments which do not require ethical compromises. Certain kinds of scientific endeavor perform better for scrutiny, but there has been a historical concern that defensive research is hampered by ethical restrictions on animal use and human subjects experimentation. This remains a concern, but the impact of new technology empowered by computation is generally to replace, reduce, and refine both animal and human subjects experiments. As a result, the technology may yet advance offensive research and permit offensive development in greater secrecy; but at the same time, it even more greatly accelerates defensive and public-health motived developments which are bound by ethical concerns – as long as those are applied in a sane fashion and not excessively. When high-content, data-rich laboratory models and methods are joined to computational methods, a much higher degree of engineering optimization can be gained from a relatively small number of animals or even animal-free microfluidic, cell culture, and organoid models.

Thank you for taking the time to listen to my ruminations on the impact computation and AI is having and will continue to have on the intentional biothreat. I look forward to hearing

the discussions and learning of your threatcasts.

Disclaimer: The opinions expressed in this paper are those of the author and do not necessarily express the position of the Navy.

Name withheld, 22 Jan 2020

Okay, I'm ready. Okay. you know, I, I'm (omitted), I'm actually associated with [inaudible] Arizona State University. So we, think about weapons of mass destruction in a different perspective. You know, a lot of times we think about, okay, so weapons of mass destruction, okay, what are different weapons of mass destruction? You know, what are the possibilities of the things that are happening in the next 10, 15, 20 years? You know, based on our knowledge and based on, you know, the access to material that they can lead to weapons of mass destruction did things, it's kind of inevitable you know, it will happen. It's just a question of when and where. So what could we do is we think, okay, assuming that it's happening, so what are the best way to respond to it, you know, and and especially many of these weapons of mass destruction are not detectable.

So you don't know you know, it's happening. Especially, you know, if you think about you know weapons of mass destruction made with the biologic in the PVL so these things are like, you know, not easily detectable. So we work towards technologies that can actually have the first responder or government agencies to be able to detect, number one who is exposed to these agents, and the number two, if somebody is exposed to a particular agent how much are they exposed to, you know, what's the level of exposure with these individuals? For example, if you think about weapons of mass destruction, it can be biological. It can be radiological. It could be explosive and et cetera. So if you think about radiological exposures you know, people are not going to be wearing, you know, a dosimeter to measure how much radiation that particular person is exposed to and how long they have been exposed so we don't know.

So for us, it's important to identify rapid detection technologies and then develop them so that we can identify, number one, who got exposed to radiation. And if somebody exposed for radiation, how much radiation that a particular person is exposed to. It's important to understand the extent of exposure. In any case, any event, if you think about radiation exposure, if somebody is exposed to very small dose of radiation you know, so you know, if they know that person is exposed to that is small dose, we can tell them that, "look, you know, are exposed to, you know, very, very, very small quantity. So you don't need to worry about it. You know, just go home, you know, get, pick it up yourself and to make sure that you go through the regular checkup with PCP like once a year, so just to make sure that, you know, nothing bad happens along the way."

But if somebody is exposed to, you know, high dose radiation you know, we need to understand exactly how much radiation that they're exposed to so we can plan their treatment. You know, anything in the mid level exposure, like, you know you know maybe, you know, two to four day range, we can give medications like [inaudible] and things like that to stimulate white blood cell production to say those individuals. But if somebody is exposed to really high dose radiation you know, we need, we may have to give them bone marrow transplantation. And in the event of radiation exposure or radiological incidents anywhere in the middle of a big city, but it's also become extremely rare. You know, if we have to give bone marrow transplantation, we won't be able to give bone marrow transplantation to everybody. So we have to have a tool to identify, okay, who needs bone marrow transplantation. You know, to whom the bone marrow transplantation may be helpful. So we have to identify exactly how much radiation that they were exposed to.

At ASU we have in developing bio dosimeters to, to to identify number one who got exposed to radiation number two, and exactly, how much radiation but they were exposed to. So we have been working on developing a bio dosimeter for the past five, six years. Recently, we have been, you know, identified by DARPA as one of the performers develop a point of care diagnostic test to identify exposure to weapons of mass destruction. And it can be a synthetic, it could be radiological, biological you know, explosives. This is kind of a test that could be used in two scenarios.

Number one let's say if a, if a first responder, a soldier comes back from a field and we think that they may have exposed to, you know one or two weapons of mass destruction agents. These kinds of point of care tests could be used to identify what kind of WMD that they had exposed. But the other scenario is let's say if a bad actor is making WMD, they have to use some of the raw materials to make those stuff. And we know using the raw material, they are constantly exposing themselves to those agents. And so our point of care test could also be used to identify you know, potentially, you know, somebody is making WMD for a certain period of time and they are exposing themselves to the precursor agents, but that use, and to make it again, so, you know, you know, what we think is that, you know, in the next probably 10 years you know in the, the, even the possibility of the WMD and [inaudible] inevitable because the, the access to these materials are like so easy. Not only access, you know the methods to, can be used to make WMD [are easily] available on the net.

And you know, so, so anybody who is interested in making WMDs can easily get access to the method and the raw materials that can be used for making WMD. So we think it's kind of inevitable as researchers, we want to be able to, you know, help in government agencies that are, going to prepare to respond to these kinds of events. You know, our focus in this area, is to make a diagnostic test widely available and easy to, easy to, use. That's what we are focusing on at ASU, at our lab.

John O'Neil, Ph.D., University of Arizona, 28 Jan 2020

So welcome and thank you all for your service. I appreciate what you're doing in the weapons of mass destruction field. I want to talk to you a little bit today about weapons of mass destruction in 2030. My perception of how those weapons are going to differ in their employment perhaps and the challenges we face in that process. So weapons of mass disruption, eclipse perceived risks from today's weapons of mass destruction in the year

2030. Today's weapons of mass destruction have a finite range of acute impacts, a finite range of probable target types, a finite range of triggering options, and a finite range of likely employment concepts of operation. This leads to attacks that are planned for specific effects. This leads also to a complicated attack vector surface with a consistent logical model. If we know the motive, if we know the means, you know, the options for delay, denial and defeat. This leads to an expensive but attractable preventive step and recovery solution performed by a limited number of largely governmental players.

But in 2030, I think weapons of mass disruption present an expansive range of acute impacts, an expansive range of probable target types, an expansive range of triggering options and an expansive range of likely employment onsets of operation. These attacks are planned for chaotic effects and chaos is a sufficient attack effect. This leads to a super complex attack vector surface with inconsistent and confounded logical models. Motive is easily cloaked. The means are not obvious and the options for delay, denial and defeat are elusive. This leads to an estimable and intractable preventive steps and recovery solutions that must be performed by a dynamic and extensive number of largely non-governmental players. So the concerns include: maintaining a focus on WMD and our community in terms of mission and resources; the need for infrastructure to support real time risk modeling in a 5g model in 5g world; need for rapid attribution of disruptive events to improve situational awareness of those that could bleed quickly into traditional WMD territory; a need for rapid assessment and triage of disinformation, PSYOPs and other distractions; a need for trusted situational awareness and liaison with many non-governmental players. And certainly there are other concerns as well. Good luck. Enjoy your exercise. I hope you succeed.

Mark C. Wrobel, Program Manager, Defense Science Office, Defense Advanced Research Projects Agency, 27 Jan 2020

Oh, so good morning or good afternoon everyone. My name is Mark Wrobel. I'm a research program manager within DARPA's defense science office. And it's a pleasure to share with you today some of my thoughts on, on this ASU threat casting workshop focused on the convergence or the intersection between cyber and weapons of mass destruction, kind of in that 10 year down the road or down the road horizon. A little bit of background about me before we kind of get into some thoughts there. So I've been at DARPA now for about 10 months. I took over a project called Sigma Plus from my predecessor who moved on. And I've come over from the Department of Homeland Security's Countering Weapons of Mass Destruction office. So I've been working in the WMD space now for close to 12 years thinking and working towards new technologies intended to be able to detect and interdict the potential use of nuclear, radiological, and now here at DARPA, biological chemical and explosive threats principally focused on the defeat of non state actors, you know, terrorists and the like.

Here at DARPA, the Sigma Plus program is all about how do we develop new advanced sensing capabilities for the full spectrum of CBRNE threats, (chemical, biological, radiological, nuclear and explosive) and do so in a manner that they can support wide deployment to monitor large geographic regions. Think large urban regions, think you know, large territories within our border regions and do so cost-effectively and yet with high performance. So we're developing a range of sensor technologies for biologic detection identification for chemical detection identification, at the parts-per-billion level, both for threat agents as well as precursors that would go into somebody, say, cooking a threat material.

And looking at how then those sensors and the data that they generate can be supported through advanced networking. So having those sensors continuously talking to a cloud analytics framework that is applying advanced analytics to the data that those sensors are generating, and then fusing that sensor data with other sources of transactional and, or, and contextual data that provides a holistic capability for federal entities and local and state law enforcement to be able to detect and interdict adversary pursuit of weapons of mass destruction. So this, this program is just into its second year now. It's a five year program. So we have quite a bit of time still to mature these capabilities. But it's a very broad and aggressive program with many different stakeholders involved in ensuring that we're building capabilities that are going to be effective and capable at the, at the end of the program.

So enough about me and the kind of the signature program that I've involved with the focus of the workshop, again, how do we look at this intersection between cyber and related cyber technologies and weapons of mass destruction and that 10 year time horizon. So if we think of cyber as information technology and the associated technologies associated with access to data potentially through, through theft and, or application of, cyber in means that allow folks to hack into systems. We can think about the potential vulnerabilities of sources of information about how WMD capabilities can be pursued and access to data and information that would allow bad actors to more aggressively develop these capabilities. When we think about the overall maturation of technologies that would enable terrorists to develop WMD capabilities, we think about technologies like CRISPR which has a significant glide path of exponential growth being applied to many of course beneficial uses.

But we can also think of those technologies as it'd be as they mature and become more available could in fact have access and be utilized for malicious intent. And we can think about that kind of across the CBRNE threat space where simply the availability of advanced cyber tools and capabilities make access to capabilities in the WMD space that much more potentially attractive and available to bad actors. We can also think about cyber in terms of where it's going, and enabling bad actors with regards to looking at how technologies that are intended to support deterrence and detection of WMD capabilities could pose vulnerabilities to those systems. And I wouldn't want to go into too much detail there, but you can think about cyber capabilities providing new tools and capabilities that allow adversaries to exploit and to circumvent various types of safeguarding and protective systems that are intended to you know, be able to detect and interdict these, these WMD threats.

So with, you know, the, these new cyber tools that could be available in the future. There is, I think a lot of promise though in new safeguards and security measures in the cyber arena that I think in the future will make it that much more difficult for bad actors to pursue WMD. We think about the advances in quantum computing and associated quantum encryption strategies that can be broadly applied. If we're looking at that 10 year timeframe to help secure these various threats that could be otherwise accessible and to overcome vulnerabilities of security systems and the like, that again, are intended to detect or interdict these threats when they're being pursued by bad actors. So, you know, on the one hand where cyber tools are that much more prolific new technologies and the cybersecurity space I think will also be available in that 10 year horizon that will provide a counter to some of those vulnerabilities. So with that I'll leave you to discuss and brainstorm within your workshop and other aspects of this intersection between cyber and WMD in the future. And I look forward to hearing the results of your workshop. Thank you.

Visit threatcasting.com for more information