The inside enemy: Weaponisation of your logistical footprint

Received (in revised form): 30th May, 2018

Brian David Johnson

BRIAN DAVID JOHNSON

is a futurist, and as such, he works with organisations to develop an actionable 10–15 year vision. His work is called futurecasting, using ethnographic field studies, technology research, cultural history, trend data, global interviews and even science fiction to provide a pragmatic road map of the future. As an applied futurist Johnson has worked with governments, trade organisations, start-ups and multinational corporations to not only help envision their future but specify the steps needed to get there. Johnson is currently the futurist in residence at Arizona State University's Center for Science and the Imagination, a professor in the School for the Future of Innovation in Society and the Director of the ASU Threatcasting Lab. He is also a Futurist and Fellow at Frost and Sullivan.

Natalie Vanatta

NATALIE VANATTA

is a US Army cyber officer and currently serves as the deputy Chief of Research at the Army Cyber Institute. Here she focuses on bringing private industry, academia and government agencies together to explore and solve cyber challenges facing the US Army in the next 3–10 years in order to prevent strategic surprise. She holds a PhD in applied mathematics as well as degrees in computer engineering and systems engineering. Natalie has also served as a Distinguished Visiting Professor at the National Security Agency.

Abstract

The intersection of digital and physical security is critical to the future security of supply chain, logistics and procurement. Considering the challenge this poses to organisations today will only expand over the next decade as the attack plan will widen fuelled by technological advances. Ultimately, the weaponisation of an organisation's supply chain (SC), logistics and procurement systems poses a significant threat to national and global economic security. This paper will provide the reader with a better understanding of the future threats and vulnerabilities emerging within the domain as highlighted through the practice of threatcasting. The threatcasting methodology can be used by organisations, companies, governments, militaries and academia to identify, model and explore these possible threats to the supply chain and logistics and procurement systems. Finally, the paper provides a series of recommendations to counter future threats at both the individual and organisational levels.

Keywords

supply chain, artificial intelligence, threatcasting, technology, adversary

Brian David Johnson
2511 NW Savier Street,
Portland,
OR 97210,
USA

Tel: +1 503-475-1891;
E-mail: brian.david.johnson@asu.edu

Natalie Vanatta, PhD
Army Cyber Institute,
Spellman Hall,
2101 New South Post Road,
West Point, NY 10996,
USA

Tel: +1 845-677-7065;
E-mail: natalie.vanatta@usma.edu

INTRODUCTION

The intersection of digital and physical security is critical to the future of security of SC, logistics and procurement. In the next decade significant advances in technology will mean that not only is the attack surface for adversaries widening but the SC itself can be weaponised. Protecting the SC and its associated systems will become an increasingly significant challenge in the future. From the edge to the centre of an organisation's logistical footprint, organisations will need to guard against both physical

and cyber threats, changing the very nature of security and threats.

The weaponisation of an organisation's SC, logistics and procurement systems poses a significant threat to national and global economic security. The very systems that are the engine of economies and the lifeline of goods and services to the world's population could and most probably will be turned against the very people and organisations that they serve. This new threat landscape and associated challenges will affect industry, militaries and governments through loss of revenue, productivity and even loss of life. This weaponisation will allow adversities whether they are criminal, state sponsored, terrorists or hacktivists to transform these systems from engines of productivity to enemies on the inside.

This paper will explore the technical advances that will drive this widening attack plain. It will highlight how the methodology and practice of threatcasting can be used by organisations, companies, governments, militaries and academia to identify, model and explore these possible threats to the SC and logistics and procurement systems. Understanding that ultimately the goal of threatcasting is to allow organisations to not only identify possible threats and then explore how to disrupt mitigate and recover from those threats. This process has clear business impacts on the future of security for the SC, logistics and procurement systems.

TECHNOLOGICAL ADVANCES

Over the next decade a constellation of technologies will bring about significant advances, disruptions and shifts for SCs and logistics, and procurement systems. Taken by themselves these advances will have a large effect but taken together the effects are multiplied.

Advancements in artificial intelligence (AI), machine learning (ML) and neural networks will allow organisations to use these technologies to increase their efficiency and productivity. Used side-by-side with an educated labour force, tasks will be automated and streamlined, generating better planning and adaptation.

Over the next decade there will be an expansion of smart things and devices. On the small scale, this is referred to as the Internet of Things (IoT) when applied to consumers and homes or the Industrial Internet of Things (IIoT) when applied to industry. Driven by the physical shrinking of computational power, sensors and communications hardware; essentially anything can be turned into a computer. These computational devices will be able to gather information, make sense of that information and then communicate it to a broader network.

On the larger scale, the effect of these advances can be seen in Smart Cities or smart environments. From buildings to houses, from warehouses to factories, from streets to entire cities — the aggregate of these technologies means that entire physical places will essentially become like smart phones. People, governments and communities will be able to customise and optimise these environments for their own values. These optimisations could include security, efficiency, sustainability or transparency.

The fuel and engines for these devices and environments will be provided by distributions of computational intelligence and the expansion of big data. Well known to many across multiple industries these two areas mean that organisations will have access to computational

intelligence wherever they might need it. From client-side devices to the cloud, from edge-servers to distributed server farms — these advances will optimise the application of intelligence and computation at the specific site where it is needed and most efficient.

Data will provide all these hardware systems with the information needed to provide the most effect. In next decade, organisations will not only continue to monetise consumer's data but also monetise unstructured data that will be generated by these smart, connected devices in IoT, IIoT, smart environments, homes and cities.[1]

For the logistical industry, the increased use of both robotics and smart mobility will be transformative. It has already been seen how robotics and automation have transformed systems like warehouses[2] and self-driving vehicles[3] but the increased normalisation of these systems to small and medium business will be a disruptive force not only in productivity but labour as well. However, smart mobility — autonomy in land, sea and air — is poised to have an even larger effect. These advances over the next decade will automate the supply chain generating great potential but great opportunity for peril as well.

NEW THREATS

These advances in technology expose a new threat landscape for national and global supply chains as well as logistics and procurement systems. The cyber threats over the last decade have generally been isolated to 'data only' threats or espionage. These types of threats were presented as data breaches for 'hack and release activities', intellectual property theft or criminal activities. Only in recent years have we begun to see the nature of these attacks change to include micro-targeting, cyber physical and cyber kinetic attacks.

Over the next ten years, threats will expand into the cyber social, cyber physical, and cyber kinetic domains as they affect supply chains, logistical and procurement systems.[4] The complex digital and physical nature of these systems mean that supply chain, logistics and procurement sit at the forefront of these changes and these threats. These systems are where the 'digital meets the physical'. Not only can traditional physical events and attacks effect these systems but these digital disruption can quickly be connected with a physical disruptions.

In this increasing threat landscape how do organisations first understand these possible threats before they emerge and in preparation for them how can they explore how to disrupt mitigate and recover from them?

THREATCASTING OVERVIEW

Helping to understand and plan for the future operating environment is the basis of a research effort known as threatcasting. Arizona State University's School for the Future of Innovation in Society in collaboration with the Army Cyber Institute at West Point use the threatcasting process to give researchers a structured way to envision and plan for risks ten years in the future. While the complexity of future can seem overwhelming, this research focuses on the cyber domain and how it can revolutionise or paralyse the future.

Threatcasting uses inputs from social science, technical research, cultural history, economics, trends, expert interviews and even a little science fiction. These various inputs allow the creation of potential futures. By placing the

threats into an effects based model (eg a person in a place with a problem), it allows organisations to understand what needs to be done immediately and also in the future to disrupt possible threats. The threatcasting framework also exposes what events could happen that indicate the progression towards an increasingly possible threat landscape.

Threatcasting is a human-centric process. The fact that practitioners participate in the modelling session is essential. Bringing together individuals from across the military, government, academia and private industry to envision possible threats ten years in the future and then brainstorming what actions can be taken to identify, track, disrupt, mitigate and recover from the possible threats. Specifically, groups explore how to transform the future they desire into reality while avoiding an undesired future.

A fundamental component of the threatcasting process is selecting the appropriate research inputs to feed the future modelling. These focus themes are selected to explore how their evolution from today contributes to the future but also how the intersection of the focus areas' growth modify each other. To select these themes, senior leaders inside the problem space and thought leaders outside the problem space are consulted on what 'keeps them up at night' or what they feel no one is focused on yet to determine the severity and urgency of the proposed themes.

When an organisation is modelling possible threats, there is a tendency to try and 'boil the ocean'. Many groups attempt to comprehend and model all possible threats. The process and framework of threatcasting ensures that groups are focused or 'curated' only on specific threat areas, so that the team can not only envision these futures but also get into the details for disruption, mitigation and recovers.

It is important to curate and find subject matter experts (SMEs) to inform and bring these focus areas possible threats within the sessions. These SMEs are individuals that can quickly describe the current state of their domain and knowledge. They illuminate how it might evolve over the next decade. They provide clarity to help participants hone and define threats in the future.

FUTURE THREATS TO SECURITY

With the expansion of technical capabilities there will be a widening of the attack plain[5] from simply 'digital only' attacks to what was seen as blended attacks. These blended attacks will cross multiple vectors including cyber/digital, social, physical and kinetic. In light of this widening attack plain, it became obvious to the US Army and military in general could not take the steps needed to secure national security and the stability of both the US and global economy by themselves. Broader steps would be needed and a range of actors will be need to work together. These participants would start with government and military but would extend into private industry, trade associations, non-profits, academia as well as private citizens. To confront the coming threats all participants would need to be empowered to take actions to secure themselves, their community, the economy and national security. A specific threat to supply chain and logistical systems can be found in the weaponisation of AI.

War on reality

While the next decade will not turn the world into the operating environment

of *Ready Player One*[6] or *Snow Crash*,[7] the world will be challenged with the definition of true reality as autonomous systems continue to evolve. Autonomous systems depend upon data to construct a model of the physical world to facilitate decision-making. If this data is corrupted or deliberately manipulated, then assembly lines, processing plants, transportation systems and procurement processes could be living in a different reality from ground truth. This could lead to widespread destabilisation. The information that is training and supporting these autonomous systems can be altered, falsified, spoofed and/or manipulated to weaken or destroy them. Done at machine speed, hidden in a wealth of data, making it difficult for humans to identify. The greater use of autonomy also means that this weaponised data can quickly move effects from the digital or cyber domain to the social, physical and/or kinetic realms.

Lack of regulation

There are few regulations that govern the use of AI and automation. Globally there is no norm or accepted practice for human oversight of these systems or how the 'human remains in or on the loop'. Our regulatory systems are not agile or adaptive enough to maintain pace with technological innovation. Therefore, the threat vector is the fact that regulations/standards/best practices for safety and security will take so long to catch up to the technology that it widens the attack surface for malicious actors.

Efficiency is easy to hack

Market forces and business management reward efficiency. Whether this is cutting costs or increasing production, both efficiency and productivity are highly valued. As these systems undergo a wave of automation over the next decade with efficiency as the driving factor, for threat actors these systems become increasingly easy to attack. If the threat actor knows how the system is constructed, what it values and what it has been optimised for — then they can use both the weaponisation of data and the use of AI to hijack and even use these systems as a part of the attack.

As an example, imagine that an organisation was first to market with an AI system poised to handle transportation routing and scheduling decisions for the movement of goods. This decision-making system had significant R&D costs associated with it. Therefore, most companies would chose to procure the organisation's system vice creating their own from scratch. Ultimately, leading to a situation where most of the market would be running the same base system. The industry must hope that every participant protects their system equally securely because a vector found in one would be a vector into all. The need for efficiency will slow down innovation, diversity, and resiliency.

Surveillance and coercion — the new insider threat[8]

No longer can an organisation just worry about those individuals that have access to their trade secrets but also those that have the 'keys to the kingdom' anywhere along the digital route that your products touch. AI will be used to find the weak link in the chain to potentially destroy your organisation's brand, product line or liquidity. Instead of the expense of hiring a legion of private investigators, forensic examiners and internal auditors — now AI can find anomalies and influence actions.

IMPLICATIONS TO SUPPLY CHAIN

These future threats are ones that the logistics field is not prepared for. What is needed is to inspire the current generation of scientists and engineers to think and innovate on this specific problem set. In times of great innovation need, we can fall back on a time-tested spark — science fiction rooted in science fact. 'All of the pioneers of astronautics were inspired by Jules Verne, and several (e.g. Goddard, Oberth, von Braun) actually wrote fiction to popularise their ideas. And I know from personal experience that many American astronauts and Soviet cosmonauts were inspired to take up their careers by the space travel stories they read as children' stated British science fiction author, inventor and futurist Arthur C. Clarke in his essay *Aspects of Science Fiction*.[9]

Based on the latest results of threatcasting research, the process of science fiction prototyping (SFP)[10] was used to develop graphic novels to inspire the current generation into developing solutions to these future problems — whether those solutions are technological, policy-based, or a combination of both.

TWO DAYS AFTER TUESDAY

Threatcasting identified a potential threat future focused on a multifaceted state sponsored terror attack against a complex automated supply chain on the east coast of the US. Starting with a targeted phishing attack at the edges of a SC system, it highlighted how a highly coordinated attack could be instigated and managed by AI instead of by a platoon of actors. More importantly, how this attack could be launched in such a way that it would be highly unlikely it would be caught and noticed in time to disrupt or mitigate its effects.

Cisco's Hyper-Innovation Living Labs (CHILL), utilised the initial threatcasting[11] findings and further explored and expanded them into a SFP entitled 'Two Days After Tuesday'.[12] The goal of the prototype was to examine possible threats to a future digital supply chain, inspiring participants in a two-day lab to seek out ways to secure this digital supply chain.

'People aren't wired to imagine the future, 10 or even five years out, which is a blocker to innovation', Kate O'Keeffe, senior director of CHILL. 'We need to create that world for them, so they can immerse themselves in this future scenario, making it immediately apparent what kind of solutions we need to prepare for that future'.[13] As a result of CHILL's 'Securing Digitized Supply Chain powered by the Blockchain', Cisco jointly invested in four to five outcomes (projects, startups) which came through the lab.[14]

11.25.27

Expanding upon the threatcasting futures and SFP of Cisco's 'Two Days After Tuesday' the Army Cyber Institute in collaboration with military officers from across multiple domains applied this weaponisation of the SC to a US military setting.

The SFP '11.25.27'[15] explored how a state sponsored terrorist group could weaponise the US Army's SC in the next decade. In this SFP the year is 2027. With the demand for increased efficiency and cost cutting measures, the government has driven towards increasing automation by utilising AI and robotics to automate the SC. With many human checks and balances removed due to cost and relying on automation to police automation, an adversary could burrow into the SC and

through a series of small nudges and modifications ensure that a train with a cargo that should never have been shipped together arrived in Seattle WA on Thanksgiving 2027.

These SFPs are being used by the Army to raise awareness to possible threats and begin conversation for how steps can be taken today to increase and ensure national security tomorrow. As technology continues to enhance military capabilities and adversaries and competitors seek to exploit vulnerabilities, these thought provoking SFPs are intended to inspire conversations about future threats.

ENVISIONING FUTURE TO EMPOWER ACTION

The goal of threatcasting is to empower individuals and organisations to take action. These dire futures full of threats and unexpected vulnerabilities enable organisations to begin hypothesising a 'whole of society' approach to dealing with these threats to SCs and logistics. For SC, logistics and procurement individuals and organisations there are specific steps that can be taken to disrupt and mitigate coming threats. SCs and logistical systems will be weaponised but if organisations take action now we can avoid many of these possible dark futures.

As an industry, SC, logistics and procurement we can place demands on technology research and development in the following areas:

- Develop algorithms that have a system of checks and balances built within themselves where decisions are optimised not only for profit but also consider ethics and societal effects;
- Implement 'kill' switches in AI which use a mechanism (digital or physical) that temporarily disables or locks the AI without destroying it completely;
- Ensure that no one entity (human or machine) has too much authority to datasets, or data warehouses;
- Develop trainings and materials to better inform and equip the industrial workforce for working securely with AI;
- Design backup systems for vetting employee data that are human-controlled and regularly checked;
- Conduct research focused on creating an AI that can evaluate decisions, monitor ethical practices in other AI systems and remain ethically compliant in its actions and decisions;
- Develop academic programmes, courses, concepts and content that include ethical behaviour when thinking about the development of AI and algorithms. Incorporate into research the implications of AI becoming highly developed and its impact on the future workforce.

Leaders of organisation in the supply chain, logistics and procurement should empower non-profit organisations to make a difference in our communities in the following ways:

- Advocate for developing national legislation that outlines data protection measures to preserve privacy and integrity of data associated with US citizens;
- Encourage industry organisations to develop standards and guidelines that support data integrity and security within the development of new digital technologies rather than as an afterthought;
- Inform the customer about the security of digital technologies that they bring into their home and family;

- Become a champion for the general public's measured and pragmatic understanding of AI.

Finally, every individual has a role to play to secure the future of SC, logistics and procurement.

- Question how your personal data is being used and the implications, both positive and negative, of sharing data;
- Trust your gut. Do not trust blindly. If something seems wrong, it very well may be. Demand that brands and organisations practice transparency and inform you of how they are using your data;
- Champion awareness with populations and communities without access to training or education about AI safety.

CONCLUSION

> 'Life is like riding a bicycle. To keep your balance you must keep moving', Albert Einstein

Protecting the SC is a notable challenge today and remains a significant challenge in the future. Where once the worry was focused on natural disasters or labour disruptions, in the future the attack surface will widen fuelled by technological advances. Therefore, SC, logistics and procurement organisations must also evolve and move forward. The barrier for malicious individuals and groups to disrupt and compromise global systems will radically shift from being resource intensive, expensive and complicated to nearly frictionless when aided by AI.

Ultimately, how do organisations prepare for these future threats? There are three basic actions that can be taken: First, education. Individuals should educate themselves, their team, and management on the threats that will arise from the evolution of today's technology and how it will be used. Second, ensure that embracing technology for efficiency reasons is tightly coupled with the risk decision on the expanding the attack plain. This is only possible if organisations truly understand the technology which is a continual moving target. Finally, become cognizant of the dual-use nature of the supply chain. Toy manufacturers never imagined that their remote control cars would become key components to detonating roadside bombs or Improvised Explosive Devices (IEDs). The SC can be reused, rehoned and reconstructed to deliver an unintended effect as well. Therefore, defending the logistical footprint of the organisation has national security effects.

Understanding these dark futures is important to the future health and stability of global supply chain, logistics and procurement organisations. But this understanding is just the first step. For an organisation to be secure and successful in the future it means that well-informed action and cross-industry collaboration needs to begin today.

REFERENCES

(1) Kugler, L. (February 2018), 'The War Over the Value of Personal Data', *Communications of the ACM*, Vol. 61, No. 2.
(2) Wingfield, N. (September 2017), 'As Amazon Pushes Forward With Robots, Workers Find New Roles' *New York Times*, available at https://www.nytimes.com/2017/09/10/technology/amazon-robots-workers.html (accessed 10th May, 2018).
(3) Yakowicz, W. (October 2017), 'Self-Driving Delivery Vans Coming to Germany Next Year', *Inc.*, available at https://www.inc.com/will-yakowicz/dhl-self-driving-trucks-germany.html (accessed 10th May, 2018).
(4) Johnson, B. D. (2017), 'A Widening Attack Plain', Threatcasting Report, Army Cyber Institute, available at http://threatcasting.com/

wp-content/uploads/2017/03/A-Widening-Attack-Plain.pdf (accessed 10th May, 2018).
(5) *Ibid*., note 4.
(6) Cline, E. (2011), *Ready Player One*, Random House, New York.
(7) Stephenson, N. (1992), *Snow Crash*, Bantam Books, New York.
(8) Johnson, B. D., Vanatta, N., Draudt, A. and West, J. (2017), 'The New Dogs of War: The Future of Weaponized Artificial Intelligence', Technical Report, available at http://www.dtic.mil/docs/citations/AD1040008 (accessed 10th May, 2018).
(9) Johnson, B. D. (2009), 'Science Fiction Prototypes Or: How I Learned to Stop Worrying about the Future and Love Science Fiction', *Intelligent Environments*, Vol. 2, pp. 3–8.
(10) Nature (March 2018), 'Editorial – Learn to Tell Science Stories', available at https://www.nature.com/articles/d41586-018-02740-5 (accessed 10th May, 2018).
(11) *Ibid*., note 4.
(12) Johnson, B. D. (date), *Two Days after Tuesday*, available at http://threatcasting.com/wp-content/uploads/2017/09/Cisco_Two_Days_After_Tuesday.pdf (accessed 10th May, 2018).
(13) Johnson, B. D. and Vanatta, N. (September 2017), 'What the Heck is Threatcasting?' Future Tense, available at http://www.slate.com/articles/technology/future_tense/2017/09/threatcasting_in_futurism_attempts_to_imagine_the_risks_we_might_face.html (accessed 10th May, 2018).
(14) Wal-Aamal, A. (September 2017), 'Cisco CHILLs about Securing Digitized Supply Chains on the Blockchain', Blog post, available at https://www.unlock-bc.com/news/2017-09-18/ciscos-chills-about-secure-digitized-supply-chains-on-the-blockchain (accessed 10th May, 2018).
(15) Johnson, B. D. (2018), '11.25.27', available at http://threatcasting.com/wp-content/uploads/2018/04/11-25-2027_high-res.pdf (accessed 10th May, 2018).