Signals and Communication Technology

Stan McClellan *Editor*

Data, Security, and Trust in Smart Cities

Springer

Signals and Communication Technology

This series is devoted to fundamentals and applications of modern methods of signal processing and cutting-edge communication technologies. The main topics are information and signal theory, acoustical signal processing, image processing and multimedia systems, mobile and wireless communications, and computer and communication networks. Volumes in the series address researchers in academia and industrial R&D departments. The series is application-oriented. The level of presentation of each individual volume, however, depends on the subject and can range from practical to scientific.

Indexing: All books in "Signals and Communication Technology" are indexed by Scopus and zbMATH

For general information about this book series, comments or suggestions, please contact Mary James at mary.james@springer.com or Ramesh Nath Premnath at ramesh.premnath@springer.com.

Stan McClellan
Editor

Data, Security, and Trust in Smart Cities

Springer

Editor
Stan McClellan
Ingram School of Engineering
Texas State University
San Marcos, TX, USA

ISSN 1860-4862 ISSN 1860-4870 (electronic)
Signals and Communication Technology
ISBN 978-3-031-61116-2 ISBN 978-3-031-61117-9 (eBook)
https://doi.org/10.1007/978-3-031-61117-9

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

Introduction

This book provides a comprehensive perspective on issues related to the trustworthiness of information in the emerging "Smart City." This area is of particular interest in a hyper-connected and online society which is increasingly dependent on digital data.

The proliferation of data, coupled with tools for manipulating, distorting, or falsifying information in ways that are difficult for human discrimination, sets the stage for a plethora of insidious societal problems. From the security of elections to the ownership of images collected on smartphones and artificially generated legal briefs, issues associated with the veracity of data are front-and-center concerns in modern society.

With a focus on the security, veracity, and trustworthiness of information, data, and related topics, the chapters address key societal issues that are affected by contemporary technologies. Issues related to AI-generated information, proliferation of disinformation, encryption vs. quantum computing, and technology trust, and related concepts are all elements of an emerging and concerning area.

These interrelated discussions are divided into three topical sections, and each chapter is presented from the perspective of industry, government, and academic practitioners who are deeply involved in specific areas of trust.

The first three chapters focus on **Geopolitics and Law**. In these chapters, experts from legal, geopolitical, and industrial sectors provide important perspectives on critical agencies, technologies, and processes that underpin trust in modern institutions. From the perspective of a Chief Strategy Officer focused on technology strategy, Amir Sternhell describes the need for resiliency in the global data supply chain, and the effect of cybersecurity intrusions as these critical facilities undergo digitalization. John Corbett discusses the evolution of law and politics in the United States from the perspective of a Partner at a leading law firm, and the role of social media in fomenting distrust in these systems. Michael McLaughlin describes the complexities of international influence in the technological and legal spheres from the perspective of a Principal in Government Relations at a leading law firm.

Chapters 4 through 6 focus on **Technology Trends.** In these chapters, experts directly engaged in cybersecurity technology supply informed perspectives on technologies, trends, and processes that are central to modern information systems. From the perspective of a seasoned technical executive and expert in data privacy, Behzad Nadji provides an overview of data security, integrity, and protection as well as regulatory frameworks and technology trends for data lifecycle management. Adam Sewall describes threats, actors, and weaknesses in critical infrastructure, including networked industrial control systems, cyber-attack vectors, and the tools used in defense and protection of strategic facilities from the perspective of a senior executive and entrepreneur in cybersecurity. Mel Horwitch discusses the concept of macro-innovation in the Smart City from the perspective of an expert in corporate strategy, policy and planning.

The final three chapters focus on trust in **Societal Issues**. In these chapters, experts from diverse areas including space exploration, artificial intelligence, and healthcare management discuss ethical, operational, and conceptual issues that are poised to disrupt key avenues of trust in modern society. Paul Bloom describes the evolution of artificial intelligence (AI) as well as the applications, issues, and ethical concerns associated with this burgeoning technology. Regina Phelps and Rodney Rohde discuss the COVID-19 pandemic in historical context, the effects and outcomes of the responses, and lessons learned from the management of widespread infectious disease. Ernest Lewis concludes with a scientific perspective on developing trust in research, data, new technologies, and unknown phenomena from the perspective of a scientist working at NASA’s Johnson Space Center.

Keywords and Concepts

- Security/Trust/Facts/Truth
- Data-Centric Security/Zero-Trust Architecture (ZTA)
- Cybersecurity/Cyberwarfare/Eavesdropping
- Encryption/Public Key Infrastructure (PKI)
- Quantum Computing/Artificial Intelligence/Machine Learning
- Supply Chain/International Relations/Distrust
- Election Security/Public Health and Trust

Contents

Part I Geopolitics and Law

Part II Technology Trends

Part III Societal Issues

About the Editor

Stan McClellan, PhD, is the Director of the JSC Engineering and Technical Support (JETS) program at Texas State University (TXST), which provides support to NASA's Johnson Space Center via subcontract to Jacobs Engineering. He was the co-Director of the Connected Infrastructure initiative at TXST from 2019 to 2023, which develops living labs and prototypes for smart grid, smart energy, smart transportation, and other smart city verticals.

McClellan is a Professor (emeritus) of Electrical/Computer Engineering at TXST, where he researches topics including Smart Grid and Smart City technologies, IP networks and protocols, embedded computing systems, communication systems, and optimization of virtualized computing environments. He was the Director of Ingram School of Engineering at TXST from 2013 to 2018.

He has held executive or senior engineering positions at companies including Hewlett Packard, Compaq, ZNYX Networks, SBE, General Dynamics (GD/FW), and LTV Missiles and Electronics Group. In 2008, he co-founded and was Chief Technology Officer for Power Tagging Technologies, a successful startup company in the Smart Grid space. He has consulted on technology and business matters for multiple companies, including Cisco, American Express, 3COM, BellSouth, N.E.T., Alcatel, AT&T, Amazon, Verizon, T-Mobile, Bank of America, Research in Motion (RIM), F5 Networks, Nortel, MCI/Worldcom, LSU Medical Center, and the US National Science Foundation.

McClellan has made invited contributions to well-known references including *Advances in Computers*, *The IEEE/CRC Electrical Engineering Handbook*, and *The Encyclopedia of Electrical and Electronics Engineering* and has authored/edited current books on important topics, including *Smart Cities in Application: Healthcare, Policy, and Innovation* (Springer 2019), *Smart Cities Applications, Technologies, Standards, and Driving Factors* (Springer, 2017), and *The Smart Grid as an Application Development Platform* (Artech House, 2017).

Part I
Geopolitics and Law

A Trusted Global Data Supply Chain

Amir Sternhell

> We believe that data is the new phenomenon. It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true — even inevitable — then cybercrime, by definition, is the greatest threat to every profession, every industry, every company in the world. (Ginni Rometty, Former Chairperson of IBM)

The global data supply chain is in transformation and in need of a reset due to a post-COVID world. This stark reality has accelerated digitization by decades, necessitating supply-chain resiliency due to greater hemispheric and regional ties. This realignment is aimed at offsetting dependency on Chinese infrastructure, manufacturing, and supplies and cybersecurity intrusions. Business-to-Business (B2B) integration remains the backbone of supply chains in which access to data files must be authorized, intended, instant, precise, accurate, and actionable to address business priorities seeking control, faster time to market, interoperability, chain visibility, and operational analytics.

New dynamic forces are also shaping things to come. Blockchains—with their immutable distributed ledgers—make it impossible to forge, revise, or delete records to facilitate full trust and transparency for customers working the chain backward. Next level Blockchains 2.0 [1] are paired with Web 3.0 protocols to establish decentralized systems on the Internet that make full use of virtual and augmented reality (AR/VR) to create a virtual coexistence for manufacturers, distributors, and customers. Open-source platforms and commercial exchanges are unified, joining operational data and off-chain interactions, and are fully auditable.

A. Sternhell (✉)
Sertainty Corporation, New York, NY, USA
e-mail: amir.sternhell@sertainty.com
https://www.linkedin.com/in/amirsternhell-91656a

S. McClellan (ed.), *Data, Security, and Trust in Smart Cities*, Signals and Communication Technology, https://doi.org/10.1007/978-3-031-61117-9_1

Data: The Lifeblood of Modern Applications

Data is at the heart of all contemporary applications. Data exists in our DNA and in the celestial mechanics of the cosmos. We pump in raw data and process it for discovery and mapping to generate the datasets that produce information, analytics, and teachings for not all data is created equal! We have the means to transform data out of an inert state—to make it smart and self-aware—resulting in "trusted party" status for Peer-to-Peer (P2P) communications and cloud-enabled architectures.

Today, decentralized data architectures are being realized. Novel meshes of individualized clouds enable data to be qualified, observable, and discoverable across the board, fostering "spot collaborations" and leveraging competencies and skills in a human-centered economy. This produces a socioeconomic compact geared for crowd-sourcing, freelancing, and an on-demand economy which establishes the individual as a branded agent. Along a lifetime of value creation, such data can be tokenized in the same manner as Bitcoins while preserving individual privacy.

Moreover, data programmed to be active and intelligent will need to withstand the challenges associated with artificial intelligence (AI) and an onslaught of natural language processing (NLP). These tools are aimed at social engineering, credential harvesting, fakes, and other manipulations in cyberspace. Such defensive capabilities for data will result in huge demand in the marketplace. The notion of being interconnected assumes that digital data will become a self-protected object to enable "Data Provenance"—tied to a unique digital ID that can also be embedded as watermark or a 3-dimensional hologram—representational of man, machine, or pictorials. Such a representation is suitable to overcome spoofing, to weed out noise, to enable the datasets aimed at training/consumption to be less biased, or to supplant what is scarce or infeasible in a digital supply chain.

The premise of this chapter is that most supply-chain initiatives—journeys conducted by the Global 2000 companies and governments—stand incomplete and remain manual and outdated. The chapter sheds light on use cases and requirements to enable an agile and visible transformation toward a comprehensive digital supply chain. The most salient aspects are explored through the platforms and tools to make a supply chain interoperable, responsive, analytical, and predictable, and end-to-end (E2E) for enterprise, military, and infrastructure applications [2].

Digitization and Convergence

We live in a world that is consumed with digitization and convergence. Technological domains associated with connected devices, AI, AR/VR, blockchain, 3D printing, 5G networks, Internet of Things (IoT), nanotechnology, robotics, space exploration, and quantum computing are growing at light speed. The pace at which technologies, processes, and businesses entwine through digitalization are leading to new intersections and opportunities for new markets, audiences, value chains, and inspiring new industries [3].

Once a process is successfully “digitalized” or transformed to a binary state, it becomes computer code and data, which is then integrated with other technologies and optimized. We must bear in mind, as well, that we are amid an emerging data-centric paradigm that is nuanced with data-layer capabilities and human-centric practices. A paradigm in which both instances can be tied to assigned universal IDs and an ever-growing identity portfolio across users, machines, devices, and workflows. This will enable greater visibility in a data-centric sphere that is nondeterministic and agent-less, and in which the balance of power is tilting to favor AI. Even today, chat-bots utilizing NLP are ubiquitous and capable of breaking the rules and Turing’s Imitation Game. This will usher in a new phase in the world of data in which AI and machine learning algorithms (ML) are baked into a supply-chain flows to enact “Decision Intelligence” [4].

These intelligent constructs incorporate a wide range of protective and decision-making techniques with the intent of authenticating, protecting, empowering, and earmarking data for domain-specific processing. Storage and cloud providers term these as secure enclaves or namespaces that share a continuous and agile protection perimeter to overcome a vulnerable blur associated with how Cloud Protective Services and Cloud Access Brokers deploy security and deal with regulations. Such namespaces can be static or dynamic, and can be aggregated in a repository for reuse in future deployments [5].

It is within these intelligent constructs where enterprises will plow their intellectual property and find adaptive practices for Industry 4.0 or 5.0 initiatives. In most cases, this outcome is defined as widespread use of connected devices at the plant/shop level and the Industrial Internet of Things (IIoT). In both instances, operational data is aggregated from sensors to create situational awareness out of unsecured devices connected to industrial systems and to the internet. This convergence between Information Technology (IT) and Operational Technology (OT) needs to contend with the addition of 127 devices per second, which complicates any notion of orchestration [6].

What is at stake, though, is a nuanced and fully protected supply chain that can originate and end on-premise, or which can be part of a hybrid cloud deployment. We have the tools, processes, and platforms, to enable organizations to exist in an environment that is server-less and keyless, while still able to overcome latency in response time to exact resiliency that is repeatable on a Just-in-Time—Just-for-Me—on an E2E basis. Further, this environment can be agnostic to the underlying infrastructure and network providers. Once a company or a consumer signals an intent to purchase, a customized cycle commences, requirements are analyzed for optimality, fulfilled, and stored for reuse.

This will entail working toward a holistic network topography and open platform which will automate the workflows, contextualize the touchpoints, enable per-customer customization, and incorporate sensor data and edge computing for situational awareness and operational analytics. Moreover, making payoffs material will require a shift from a cost-basis mentality, tied to a siloed and disparate supply chain, to a more distributed hub-and-spoke design.

Such an environment will make data ingestion more granular and far reaching while enabling supply chains to advance and position themselves as profit centers. Consequently, supply chains become mission multipliers that monetize data by generating feedback loops to optimize via “Big Data” or to triangulate toward research and development (R&D), fulfillment, and innovative processes.

Pace of Innovation and Data Growth

In his book “Chip War,” author Chris Miller describes how in 1965 Intel’s founder Gordon Moore postulated that the number of transistors double in an integrated circuit—while costs of computers drop inversely by such—every 2 years. This came to be known as Moore’s Law and an accepted reference to qualifying exponentials, acceleration, and disruption, in framing much of the world’s progress in semiconductors and IT and its impact on the domains [7].

The pace of innovation over the past 60 plus years has swayed from a linear mode of progression—in which the increases in performance equate to the same amount over time—to exponential growth in which yields and trajectories increase very rapidly over months. Advances in hardware and software engineering have spurred quantitative leaps forward in performance which is measured in the billions. Consider such an advance in the case of the Apollo 11 mission that guided a capsule to land on the moon, in 1969. This mission used 62 bytes of random access memory (RAM) per kilogram of hardware. In contrast, today, a two-kilogram laptop computer comes equipped with 64 gigabytes of RAM.

Growth in data has not stood still either. Data management has been around for four decades. What started as centralized data warehouses, structured data, data dictionaries, and data metrics has blossomed—due to Moore’s Law and a general move to “digitalization”—to data exchanges, markets, and edge technologies, replete with algorithms and artificial general intelligence (AGI) and the utilization of generative AI chat-bots able to comprehend, learn, apply, and change the limit of possibilities.

The amount of data created, copied, and consumed globally today is around 100 zettabytes or a trillion gigabytes. Data is growing around an average of two zettabytes a day due to a rise in user activities in Meta, Google, Amazon, and Microsoft as well as AI/ML and Deep Learning constructs, which require a continuous consumption of vast volumes of data for activities such as large language modeling.

The current global supply chain is projected to grow to 200 zettabytes by 2025 with 55.7 billion connected IoT devices generating 80B zettabytes of data [8]. Businesses collect about 2.5 billion gigabytes a day of which most of it is attributed to customer data that jump-starts a production environment. This invokes an on-demand cycle that aggregates huge volumes of data which are mined by AI/ML for analytics. Such outcomes are transforming the world of retail, health, entertainment, transportation, energy, and education.

Hence, an enterprise data supply chain gets its cue from the processes and workflows involved in a manufacturing supply chain, as diagrammed in Fig. 1.

The distribution of products and services to consumers equates—whether by land, sea, air, rail, and autonomous/unmanned—to a data lifecycle that propagates and procures data and turns it into a consumable product. The schema in Fig. 2 describes the processes that turn raw data into useful information and actionable

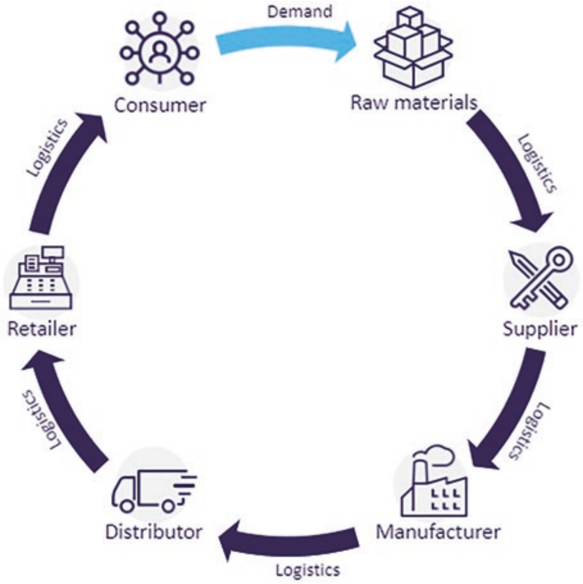

Fig. 1 Manufacturing supply chain workflow

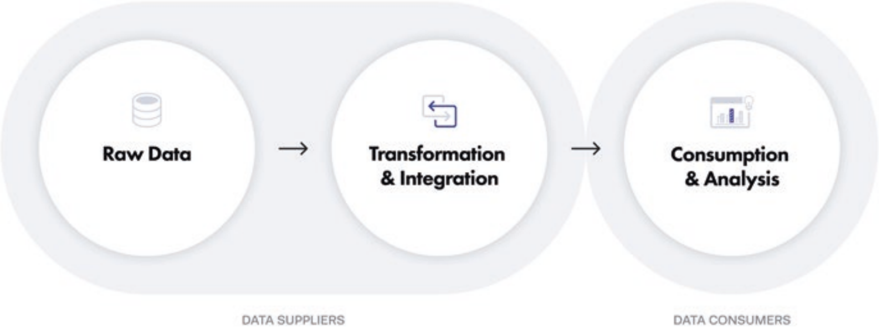

Fig. 2 Data suppliers and consumers

insights. This process is defined as: *Input* > *Output* > *Processing* > *Storing* > *Cont rolling*. In this fashion, enterprise digital supply transformation is comprised of the building blocks associated with the way we map, integrate, comply, mitigate supplier risk, and trace, automate, decarbonize, analyze processes, enabling smarter-visible workflows to rethink businesses [9].

Supply-Chain Dependence

All told, a supply chain is reliant on Business-to-Business-to-Consumer (B2B/B2C) integration—which can coalesce multisuppliers. This process is driven by data sharing adapted to shifts in a business environment and a supply-chain infrastructure.

For processes to interoperate, software developers and integrators use an application programming interface (API) to provide asynchronous or synchronous communication between two applications. This interchange synchronizes the scenarios and goals for automation and real-time response.

As such, APIs are prone to hacking and manipulation since they provide easy access to data or user sessions. This means that an API can be exploited over and over once malware has been injected into it. Such exploits may become undetectable to virus scanners and can remain as an advanced persistent threat (APT). An APT instance may change its own code when it replicates itself to remain under the radar, ready to fake user IDs and multifactor authentication (MFA), steal passwords, and commit denial of service (DOS) attacks. Once compromised, account privileges are escalated, and the penetration continues into networks, operating system (OS) resources, devices, sabotaging on premise or cloud-based workflows, and opening listening posts for adversarial AI to sift for critical data [8].

What aggravates matters further is the fact that much of the theft relates to industrial espionage associated with gleaning competitive intelligence from shipping documents—such as the carrier, cargo owner, freight forwarder, fleet manager, bill of lading—that are transmitted by electronic data interchange (EDI) originating at the manufacturer and ending with the destination. EDI has been a standard in automating the transfer of applications between computers directly for the past 60 years. This legacy is primed for a new data-layer remake and a data provenance standard bridging privacy, probability, visibility to inventory, shipments, and sales.

Supply-chain disruption is the new norm! The geopolitical arena has become rife with dominant actors such as China, Russia, Iran, Turkey, and North Korea, which are following policies aimed at preserving dictatorial regimes and theocracies. Supply-chain piracy has been exposed to events such as COVID-19, the shortage in semiconductors, Ukraine War, and the latest War in Gaza. Coupling these matters with the fact that China is building roads, bridges, rail, for much of the world and emerging countries and owns most of the world's maritime infrastructure, its shipping companies, and ports, which is creating uncertainty and ambiguity for the west regarding the entire manufacturing supply chain.

China is in the process of building a digital silk road. It has asserted itself as the global leader in 5G networks and is engaged in a back-end strategy of seeking control of the world's telecom/wireless/device infrastructure to germinate data colonies with the purpose of ingesting volumetric data earmarked for AI training for both military and commercial use. It is a regime that seeks to exploit the openness of democratic systems as to undermine the west's competitiveness through industrial espionage and intrusions to sabotage our institutions and infrastructure (along with Russia, Iran, and North Korea) [10].

This is spearheaded by the People's Liberation Army (PLA) premier hacking Unit 61,398 that has inflicted damages to the United States in the trillions of dollars (attributed to stealing the prototype's for the US Air Force F22, F35, C-117, and the Naval Aircraft Carrier Gerald Ford) through well-placed APTs-focused malicious cyber activity. The PLA's aim is to penetrate and prolong network/system intrusions within institutes, national labs, and the military-industrial complex. In 2012, Keith

Alexander, former head of the US National Security Agency (NSA), deemed China's theft as the greatest transfer of wealth in history. There are 42 known APTs that exist today [11].

Consequently, the United States and its allies, in regions other than Brazil and India, have been on a path of deglobalization to undo the interdependencies and integration in certain parts of the world and with China, in particular. "For too long as a nation, we haven't been making the big and bold investments to outpace our global competitors" declared President Biden to multiple corporate CEOs, while he admonished them for falling behind on R&D and manufacturing [12].

This has ushered in a mind-shift in US policy that can be captioned as "The West and The Rest." The broad implications have led the Biden Administration to impose a choke on China and to earmark over a trillion dollars for the Infrastructure Investment and Jobs Act (IIJA) [13] with the intent of bringing back manufacturing home while upgrading the electric, power, and water grids, broadband, highways, waterways, freight rail, airports, seaports, public transit, and electric vehicles. This approach aims to make US supply chains domestic/hemispheric, protected, and resilient. In a word, "Made in the USA" in its 2.0 rendition is attributed to a mix of steady domestic and selected foreign suppliers to stabilize and groom an effective supply chain for multiple industries.

Special attention was given to the semiconductor Industry—as part of the US restrictions on China's access to chip technology and its embrace of Taiwan's TSMC—through the Decadal Plan for Semiconductors [14] and ensuing CHIPS Act [15] to incentivize industry with $300B to embed semiconductor technology into emerging technologies. In essence, enable and seize futuristic opportunities in the intersections associated with AI, Quantum Computing, advanced wireless 5/6G technologies, and Low Power Wide Area Networking (LoRaWAN) that are the communication backbones of IIoT. Thereby, secure locally made supply of semiconductor chips for national security and critical infrastructure that promise incalculable societal benefits.

Moreover, in "Chip War," Chris Miller posits that during COVID-19 certain types of chips became difficult to acquire due to remote work from home necessitating more servers to absorb the rise in online and virtual activities. This was coupled with global shortages in logic (processors, controllers) and ICs widely used in industries, manufacturing, and automobiles, along the tenets of Industry 4.0 [7].

There are, currently, over 25,000 supply chains which constitute a 13-fold increase since COVID-19 started [9]. Much of this growth may be attributed to operational requirements for a dynamic data exchange along unified data definitions. These requirements include information and database sharing and open APIs to transmit inventory and fulfillment data accurately, timely, and securely through EDI or any other P2P legacy system. Moreover, much of the transformation has come about from a reset of suppliers that cater to on-demand/just-in-time delivery, source proven new and renew old manufacturers, and mitigate sovereign risk.

Such nation-state level exposures are challenging our freedoms to navigate in a world in which China has commercial and military domain over strategic ports and routes; Russia's War in the Ukraine; Iran's aggression in the Middle East which has