JIFM JOURNAL OF INSURANCE AND FINANCIAL MANAGEMENT

Beyond Data Protection to Command and Control (C2) Sustainability in a Post-COVID19 World:
Execution of U.S. Data Protection Act for U.S. Data Protection Agency; U.S. Data Protection Act Proposal by US Senator for New York Kirsten Gillibrand

Dr. Yogesh Malhotra [a,*]

[a] *www.YogeshMalhotra.com : Global Risk Management Network, LLC, New Hartford, New York 13413, U.S.A.*

ARTICLE INFO

Article History

Submitted	21 Dec 2022
Accepted	23 Dec 2022
Available online	16 Jan 2023

JEL Classification

A, C, E, G, P, Z, A1, B23, C00, C01, C02, C4, C5, C6, C8, C9, C10, C11, C12, C13, C14, C15, C18, C19, C22, C32, C40, C45, C50, C51, C52, C53, C55, C58, C60, C61, C63, C69, C87, C93, D7, D8, D70, D71, D74, D80, D81, D82, D83, D84, D89, F1, F3, F30, F4, F40, G1, G12, G2, G11, G12, G20, G22, G24, H56, K00, L5, L50, L8, L9, L63, L86, L96, L86, M15, M21, M41, M42, O3, O31, O32, O33, P4, P40

Keywords

Risk Management
Command & Control
Adversarial Command & Control
Counter-Adversarial Command & Control
Survival & Sustainability
Systems
Cyber Security
Network Security
Pandemic
COVID-19
Coronavirus
Contagion
Cascading Attacks
Data Protection
Data Protection Act

ABSTRACT

The current article about execution of the Data Protection Act (DPA) proposal was sent a week before the State of New York state wide shut-down due to the global COVID-19 coronavirus pandemic to Senator Kirsten Gillibrand, the US Senator from the State of New York who had proposed the DPA. The article underscored the need to advance the focus of its execution beyond *ex-post* reactive penalization of respective firms for compromise of privacy of personal information by firms 'storing' such data to focus on *ex-ante* Sustainability and Survival material to individuals. There were two specific issues underlying the above recommendations. First, it is not just about storage of such 'entrusted' data but if and how such data was 'exploited' by the trusted firms to *Command & Control* the *Survival and Sustainability* of respective individuals. Second, in most cases, those firms may not even be responsible for such compromise of individual data entrusted to them given that they are themselves subject to being 'hacked' by third parties. Hence, to solve the more *critical systemic problem* encompassing all individuals and firms, we need to build and stress-test systems to preempt and prevent such 'hacking' attacks in addition to the proposed normative compliance measures. Essentially, for Sustainability and Survival of individual Command & Control (C2), we need to focus on developing and deploying Adversarial C2 systems to stress test the robustness of C2 systems as well as Counter-Adversarial C2 to counter the adversarial threats.

The specific focus of *global networked systems, infrastructures, and networks* that can get impacted in *global systemic exponential cascading attacks* given the inter-connectivity of networks and often endogenous nature of such attacks was compared with analogous *global contagion risks* of COVID-19 and their global and national 'spread' that all are monitoring. Over the subsequent few weeks, the COVID-19 global pandemic had unfolded with major adverse impacts evident across public health, global financial and economic, and, global geopolitical, national defense and security, and, related socioeconomic domains. The Survival & Sustainability of Systems at all levels which is at stake and the respective critical significance of Command & Controls - spanning global, national, organizational, individual, and, even human cellular levels of analysis – are being recognized worldwide as never before on the COVID-19 pandemic threats and vulnerabilities "global theater". The respective role of such Command & Controls that are the most essential defining attributes of all *Self-Adaptive Systems* and their *self-identity*, *self-regulation*, and, *self-determination* are also being recognized in terms of determining the Sustainability and Survival of the respective Systems at all levels. For preempting and preventing future similar global threats such as COVID-19, we need to develop and deploy Adversarial C2 systems to stress test the robustness of C2 for respective Systems as well as Counter-Adversarial C2 to counter the adversarial threats. Our Global Post AI-Quantum, Finance & FinTech, Command & Control Network ventures, United States Air Force (USAF) Air Force Research Lab (AFRL) Commercialization Academy ventures, AIMLExchange.com, BRINT.com, and C4I-Cyber.com fulfill the above global missions.

Journal of Insurance and Financial Management

*Corresponding Author:
Dr.Yogesh.Malhotra@gmail.com

Author(s) retain copyright of the submitted paper (Please view the Copyright Notice of JIFM).
© Dr. Yogesh Malhotra, www.YogeshMalhotra.com. All Rights Reserved, 2022.
This work is licensed under a Creative Commons Attribution 4.0 International License.

Thank you for sharing your vision of the U.S. Data Protection Act and the Data Protection Agency in your article "The U.S. Needs a Data Protection Agency."[1] I am excited about your proposal having founded the world's largest Digital Transformation Network of practices guiding worldwide Digital practices for U.S. and global firms and governments since over 28-years ago[2]. In the attached proposal document, we provide actionable and specific execution advice and recommendations for the execution of the U.S. Data Protection Act for the Data Protection Agency to help enable the USA to lead Data Protection (DP). We include actionable recommendations to enable USA to lead Data Protection by advancing *ex-ante* and *proactive* Data Protection to complement the current legal regulatory compliance framework. Additionally, we present a reader-friendly overview of Network and Computer Security Engineering issues material for legal and regulatory agencies to help advance our guidance of the U.S. Data Protection Act. For execution and implementation of the proposal, we introduce the New York State tech ecosystem of the United States Air Force Research Lab (AFRL) and our associated Air Force Research Lab Commercialization Academy (CA) ventures. The AFRL-CA ventures founded by our New York State venture capital firm, Global Risk Management Network, LLC, are pioneers and leaders of related global R&D and applied industrial practices in Data Protection and Risk Management. With IT Security, Risk Engineering, and, Risk Management leadership practices spanning critical National Information Infrastructure and Global Information Infrastructures and Banking & Finance, Computer Software, Defense & Space, Government, Healthcare, Information Technology Services, Internet, and, Network & Computer Security industries since early 1990s, the Global Risk Management Network, LLC is a global worldwide leader advancing the USA as a leader in Data Protection. We look forward to collaborating with you and others in the DP mission.

Original draft of the proposal document prior to journal submission and review is available at:

https://www.yogeshmalhotra.com/DataProtectionAct.pdf .

Social Influence on the WWW, Digital Self-Determination, & Shoshana Zuboff's 'Surveillance Capitalism'

It is of interest to observe that other scholar-practitioners of Digital Self-Determination such as Shoshana Zuboff[3] have endorsed your Data Protection Act to found a new independent agency, the Data Protection Agency (DPA), tasked with protecting consumer data. Having published the earliest empirical field research on Digital user's self-determination and social influence (IEEE-HICSS[4]) in course of Top-10 IT PhD (1998) from the University of Pittsburgh, I have both built upon and advanced Professor Shoshana Zuboff's research (*ACM*[5], *AMCIS*[6], *JMIS*[7,8]). My above empirical field study on Digital 'Social Influence' Networks for the Top-10 IT PhD preceded Professor Shoshana Zuboff's recent book on *Surveillance Capitalism* critiquing Facebook's social influence studies by more than two decades. The Digital research methods and models I developed in above studies are applied by global organizations such as NASA[9].

The Crisis of Data Protection & Data Privacy is In Fact a Crisis of 'Command & Control' of Lives and Nations

While working on PhD, I also founded world's top Digital site (Computerworld) adopted and recommended by global IT leaders such as Microsoft founder Bill Gates[10] and sought by world-leading tech firms such as IBM, Intel, and, Google to launch IPOs and new IT services in Digital practices we pioneered[11]. I built the world's go to Digital resource (e.g. editorial review

by Fast Company[12]: "If @BRINT doesn't have it, then you probably don't need it.") as one of the world's Top-20 or so sites with the beginning of the WWW. Hence, I can very well relate to how a tech firm such as Google, which sought and procured our Digital Social Network 'portals' for channeling their online advertisements prior to 2004 IPO, transitioned to 'building major empires of data with information about our private lives' – as you state in your article – among other target firms of your Data Protection Act (DPA). As you note in your article, Digital consumer's "very existence is being parsed, split, and, sold to the highest bidder" often in order to 'command and control' individual's very lives and existence. As evident from headlines on social media influences to influence national elections[13] of multiple nations, such 'Command and Control' may not only 'influence' and control individual lives but also 'Futures' of nations and national leaders such as by 'algorithmic control' via social media[14].

DPA: Beyond Data Protection & Data Privacy to Privacy Enhancing Technologies (PETs) and Deep Fakes

Your Data Protection Act (DPA) is welcome news for Digital consumers such as myself being one of earliest Digital consumers, practitioners, scientists, and, technologists credited by *CIO Magazine* as a Digital pioneer. See for instance, my interview published in the *CIO Enterprise* of September 15, 1999, conducted by the *CIO Magazine* journalist in course of my invited keynotes to the San Francisco Bay Area and Silicon Valley Tech CEOs and Venture Capitalists https://www.BRINT.org/DoesKMeqIT.pdf. Its subsequent reprint is in the *ITWorld Canada* issue of January 31, 2000: https://www.itworldcanada.com/article/intellectual-capitalism-does-km-it/33754. In that CIO interview, I had encouraged Digital CEOs to advance beyond the mainstream focus on *historical* "Data" to post-WWW era "*Anticipation of Surprise*" (https://www.yogeshmalhotra.com/publications.html) *future-oriented* focus on **Controls** as already adopted by our world-leading BRINT® Global Digital Transformation Network (www.BRINT.com) clients such as Goldman Sachs https://FutureOfFinance.org/.

I can readily identify with your point that consumers "deserve to be in control of your data" and "need a way to protect yourself" from companies that "monitor their activity" and apps that contain "backdoor access to all of phone's data." Having built Digital practices for NSF, UN, U.S. and worldwide governments, New York State (NYS), and world's largest IT, Banking & Finance firms including Wall Street investment banks with $1 Trillion AUM, I can relate to your points about Digital consumer's Data Protection. My recent Digital Networks, Practices, Technologies, and Ventures advancing Internet, WWW, Network & Computer Security & Privacy Enhancing Technologies (PETs) and AI-ML-Deep Risk Mitigations disseminated via the AFCEA C4I-Cyber Conferences sponsored by the AFRL, and, New York State Cyber Security conferences[15,16,17,18] advance beyond *ex-post* 'Data Protection', such as Data Protection and Risk Management for Global, National, and New York State Banking & Finance industries among others, to *pro-active ex-ante* 'Command and Control' focus (see, C4I-Cyber.com, for instance). So have my recent Networks, Practices, Technologies, and Ventures disseminated via the Princeton University[19,20,21] conferences sponsored by firms such as Goldman Sachs and Citadel, as well as AI-ML-DL-NLP-RPA industry expert leadership of 1.000 global worldwide Management & Leadership industry executives for the MIT Computer Science & AI Lab and MIT Sloan Management & Leadership programs[22]. Also, my CEO-CxO teams' leadership for global AI-ML-Block Chain-Cloud Computing pioneer CEO teams has focused on 'network-centric computing' PETs such as differential privacy, homomorphic and semi-homomorphic encryption advancing beyond to Cloud-Native PIP encryption[23,24,25,26,27].

Monitoring, Intelligence, Surveillance, and, Reconnaissance of Data Control Survival and Sustainability

"Companies and foreign adversaries want to exploit your data. Someone should be looking out for you." I strongly identify with the spirit of your stated mission of the Data Protection Agency and the Data Protection Act. I have advanced practices on both competitive and business intelligence earlier (e.g. of global honors include Leaders and Legends of Business Intelligence & Data Warehousing, 1998) and for C4I-ISR[28,29] (Command, Control, Communications, Computing, and Intelligence - Intelligence, Surveillance, and Reconnaissance) more recently while serving as Chief Scientist on the United States Air Force (USAF) Pentagon CTO-DoD CIO senior advisor team with USAF Secretary and Joint Agency Artificial Intelligence Center (JAIC) as clients. Hence, I can relate to your points about the blatant surveillance such as in case of a "fitness app" used to "monitor your heart rate" with data being sold to third parties. A more sinister case could be that of a heart pacemaker that can be exploited given known or 'zero day' vulnerabilities in software, hardware, firmware, or semiconductors to literally control life and death of respective patients. As we shall see in the following discussion, the key concern for Data Protection needs to be and should be thus recognized in terms of *survival* and *sustainability* not only of individuals but of our nation as well as critical National Information Infrastructures, Global Information Infrastructures, as well as all networked commercial and other enterprise activity.

How can the USA Take the Lead in Data Protection: By Using Nuanced Understanding of "Adversaries"

You note that "the United States must make an effort to take the lead and do something about data protection." Having served on 32 national expert panels of Computer Scientists for the U.S. National Science Foundation to allocate multi-million-dollar SBIR/STTR grants for commercializing U.S. IT Cyber Computing & Cyber Security innovations, it will be my privilege to assist you and your key stakeholders in the above national DPA mission as an IT AI-Engineering-Security-Cloud Computing Professional-Architect with Top-3 DoDD 8570 IT Security certifications[30] (CEng, CISSP, CISA, CEH, AWS-CCP, AWS-CSAA)[31]. As discussed in my Quantitative Finance-Computer Science-Network & Computer Security Engineering post-doctoral thesis[32] (2015) – reviewed by the committee of senior Computer Scientists leading Air Force Research Lab (AFRL), New York State Cyber Research Institute, and, the State University of New York (SUNY) – we need a more nuanced understanding of "adversaries" given "insider threats"[33] wherein 'insiders' – intentionally or [most often] inadvertently – may themselves become participants in adversarial exploitation of their own data or devices on their own and other [provider] networks and/or [more often] on individual [mobile] devices such as smartphones. The situation is analogous to that of coronavirus COVID-19 wherein patients become unwilling participants in the spread of contagion risks[34].

How can the USA Take the Lead in Data Protection: By Focusing on *Pro-Active* & *Ex-Ante* Data Protection

By bridging the worlds of Wall Street hedge funds and USAF-Research Lab National Defense and Homeland security, the above Network & Computer Security thesis built original integrated understanding of global Cyber and Financial-Economic risks and risk management that are now subject of mainstream media headlines[35]. It relates to the core thesis of Professor Zuboff's work and your DPA in how the financial and economic motives of specific Big Tech

firms have perversely and adversely resulted in the exploitation of data entrusted by digital users and consumers to those companies. Given so, the specific punitive measures introduced by the DPA may seem logical to prevent such perverse profit-chasing by such Big Tech (and other) firms who may sacrifice consumer interests based upon obfuscated blanket 'opt-in' 'permissions'. Above legal measures have demonstrated limitations, being *reactive* and *ex-post*. They may not necessarily result in preferred DPA outcomes as evident from many such enforcements that have left a trail of *ex-post* 'legal settlements' given absence of *ex-ante* 'permissions' because the financial penalties are often a trivial fraction of economic profits. Given the nature of the Digital technologies, above measures may not really yield *pro-active* and *ex-ante* Data Protection improvements or ensure *pro-active* and *ex-ante* Data Protection.

How can the USA Take the Lead in Data Protection: By a Sophisticated View of "Data Protection" and PETs

The following analysis underscores how USA can lead Data Protection by advancing beyond *ex-post* and *reactive penalization* for *lack of Data Protection* to *ex-ante* and *proactive* Data Protection improvements.

As outlined above, punitive measures may not advance Data Protection beyond 'misuse' of entrusted data by service providers, such as in the contexts of [intentional or inadvertent] adversarial exploitation by adversaries – domestic *and* foreign, insiders *and* outsiders, and, oneself [given insider threats] *and* others. In addition, the proposed Privacy Enhancing Technologies (PETs) may deter the Big Tech's exploitation of Digital consumer data for profit, however, they may still not yield Data Protection. There are diverse multiple layers of such PETs across organizational IT Systems, Infrastructures, and, Networks as someone in InfoSec leadership role would recognize, as I did in CISO role leading and serving as invited expert for NYS IT and Networks Administration. Similarly, anyone who has invested thousands of hours leading and conducting *penetration testing*[36] of Systems, Infrastructures, and, Networks in authorized Darknets and, built and delivered State-accredited *Offensive* and *Defensive* Network & Computer Security+ professional certification programs would recognize likewise, as I do.

From a 'network-centric computing' perspective, the problem with PETs is that it is not a specific technology *but* the weakest links in the network that get most easily exploited. Many of the latest technologies including AI, Quantum, IoT, etc. may often include such 'weakest links' resulting in their exploitation. Our AFRL-CA ventures such as AIMLExchange.com, BRINT.com, and C4I-Cyber.com have in recent years been building global *AI-ML-Quant-Cyber-Crypto-Quantum-Risk Computing* awareness of such multi-dimensional and systemic threats and vulnerabilities in addition to building and advancing specific Networks, Practices, Technologies, Teams, and Ventures toward *pro-active* and *ex-ante* mitigation of related AI and Quantum Risks[37]. Such weakest links can result from digital social network behavioral issues related to *insider threats* such as a network, system, or devices user clicking on a phishing link or opening a malware attachment, or, digital social network *usage* issues such as drive-by-download attacks[38]. Such 'weakest links' can also result from *zero-day* and other attacks such as Meltdown and Spectre that exploit critical vulnerabilities in Intel and AMD processors which may be 'difficult to fix' but may allow remote code execution and control of computers, devices, and, infrastructures by distant adversaries[39]. Such specific threat vectors and vulnerabilities result from cyber risks being unique, particularly, in being different from

financial risks which are typically better understood by many legislators and regulators given familiarity as discussed in the Network & Computer Security thesis[40] (Malhotra, 2015):

p. 15: "…Unlike other risks, cyber risk poses a uniquely different set of exposures as it is intertwined with the medium and the message in the increasingly digital world of networked communications. While in case of cyber risk exposure through spear phishing and whaling, the exposure is through the specific users (decisions to click on a link, for example) reading the message. However, the more significant and latent cyber risk is in the inherent and potential vulnerabilities in the enabling medium such as the underlying operating system or networking software. For instance, the vulnerabilities inherent in the medium can be exploited resulting in cyber risk regardless of the user's actions or inactions."

p. 15: "…From trust computing perspective, every component of software, hardware, firmware, or networks that interacts with any other upstream or downstream second-party or third-party provider, vendor, or contractor is vulnerable and exposed... Given known infiltration and compromises through spear phishing and whaling at the most senior echelons of world governments and global firms, no one is safe including heads of governments and heads of corporate firms."

p. 16: "…Once compromised, any such trusted user regardless of the status on the respective hierarchy can become the channel of contagion that can compromise the complete network of trust as well as all other trusted users on those networks. Taking the process a step further beyond inter-enterprise focus to intra-enterprise focus, any compromised trusted network can become the channel for infiltration of the trusting network. Hence, across diverse networks, any entity or device trusting any other network which can be compromised can become potentially vulnerable and after being compromised become a carrier that can result in other devices being compromised. Once compromised, the exposed network, device, and/or entity serves as a channel for transfer of economic value or destruction of economic value in the online cyber war game." [One can see the eerie analogy to the ongoing COVID-19 contagion risk herein.]

p. 17: "A key challenge is determining the real identity of the device or the network as the source of attack by tracking it precisely across the various intermediaries, willing or unwilling, knowing or unknowing, involved in the attack. A more complex and convoluted challenge is knowing even if the authorized users or owners of those specific devices or networks actively participated in the attack or even knew about the attack before or when it was launched." [Such 'community spread' phenomena may bear an eerie resemblance to the current state of diagnosis and detection being used to contain COVID-19 contagion[41].]

p. 16-17: "Regardless, from the above analysis, it follows that everyone is a potential target, potential accessory, or even a potential source of attack, even when they are unwilling or unknowing participants in any given attack or a 'network of attacks'. Merely detaching oneself with an air gap from all networks and devices does not necessarily preclude an actor as a potential target, accessory, or, source of attack, not considering RF signals. As long as the agent or device can communicate with, i.e. pass on a digital message to, other agents or devices who are not detached or who can communicate with other agents or devices, it could be plausibly potential target, accessory, and even a source of attack."

Based upon above analysis, the USA can lead global Data Protection standards and align with other global-national Data Protection and European GDPR standards by advancing beyond *ex-post* and *reactive penalization* for *lack of Data Protection* to *ex-ante* and *proactive* Data Protection *Command-and-Control* improvements[42] which is specific focus of C4I-Cyber.com.

How can the USA Take the Lead in Global Data Privacy, Protection and Sovereignty Standards: By Using Zero Trust Architectures and Penetration Testing

Above analysis and discussion highlight how Data Privacy, Protection and Sovereignty focus on *ex-ante* 'symptoms' of the more serious *ex-ante* 'Command and Control' 'crises' associated with *survival* and *sustainability* of individuals, groups, enterprises, and, nations. As discussed, the DPA is currently framed to ensure regulatory compliance by penalizing an enterprise's non-compliance ex-ante as evidenced from specific Data Protection violations. As observable from recent precedents, such as FTC's $5 billion fine imposed on Facebook for alleged data abuse, such measures have effectively done "little to restrict the company from misbehaving in the future.[43]" Also, as evident from the above global industry analyses, the USA can lead Data Protection by advancing beyond *ex-post* and *reactive penalization* for *lack of Data Protection* to our outlined *ex-ante proactive* Data Protection measures as discussed herein. The explained 'problems' of Digital Command & Control are often intertwined with the issue of Digital Trust given that the Internet technologies are built on the foundation of 'Trust all' by default[44].

The Zero-Trust model is a possible solution for the above problem inherent in the fundamental technical foundations of the Internet as observed in my post-doctoral Quantitative Finance-Computer Science-Network & Computer Security Engineering thesis[45] (Malhotra, 2015):

p. 17: "Zero Trust is an alternative security model that addresses the shortcomings of failing perimeter-centric strategies by removing the assumption of trust. With Zero Trust there is no default trust for any entity—including users, devices, applications, and packets—regardless of what it is and its location on or relative to the corporate network."

p. 18: "For example, the Internet-of-Things opens up a whole new set of vectors of cyber risks and potential cyberattacks. Zero trust approach, relying upon trusting no-one consistent with the above analysis, assumes that the traditional perimeter based security will be breached, including all defense-in-depth security layers, and hence valuable data and assets need to be protected from inside-out. Zero-trust approach would therefore include advanced data protection such as encryption, data cloaking, data masking for all critical data assets, both at-rest and in-transmission. It can be deployed in addition to 'adaptive perimeter' approach to minimize the attack surface vulnerable to more sophisticated cyber- attacks. Examples of adaptive perimeter include using application wrapping to encrypt data-in-motion from mobile apps across the cyberspace and connecting authenticated mobile users into secure communities of interest, and, wrapping applications on the mobile devices."

Such zero-trust architectures are enhanced by *penetration testing*[46] of related Systems, Infrastructures, and, Networks wherein respective owners themselves conduct the type of attacks ("Hack Yourself First") expected from adversaries to stress test their own systems and networks. Related systems and networks penetration testing capabilities are now integrated in multi-function technologies such as the Unified Threat Management (UTM) systems that integrate capabilities of prior Firewalls and Intrusion Prevention & Detection Systems (IPS/IDS). Examples of diverse Access Controls and related Encryption and Authentication

mechanisms across diverse defense-in-depth layers represent the diversity of PETs as listed in the synopsis of my earlier NYS IT Security leadership[47] role. Given that adversarial techniques are often deployed for penetration testing of own systems, infrastructures, and, networks, specific penetration tests focused on adversarial takeover of command and control can thus be characterized as Adversarial Command & Control (AC2) techniques and methods.

How can the USA Take the Lead in Data Protection: Command & Control (C2) Supremacy for Key Technologies

The 'problem' of 'Command and Control' associated survival and sustainability discussed above has been quite evident in the form of attacks such as distributed denial of service (DDOS) attacks, ransomware attacks, and crypto attacks often launched using inexpensively rented botnets in recent years. With the emergence of advanced technologies such as Artificial Intelligence, Machine Learning and Deep Learning; Block Chain & Cloud Computing; and, Quantum Computing and Quantum Cryptography, we are seeing rapidly evolving threat landscapes as well as vulnerability landscapes[48]. Homeland security and defense intelligence operations are contemplating security from networked swarms of drones (UAVs) such as by use of counter-drone systems. In respective cases, such as of botnets and swarms, the most crucial capabilities to pre-empt and prevent such threats are that of Command & Control (C2), in particular, Adversarial Command & Control (AC2), and, Counter-Adversarial Command & Control (CAC2). For instance, use of drones for adversarial purposes is an example of AC2 and use of counter-drones to safeguard from such drone attacks is an example of CAC2.

Why Command & Control (C2) Supremacy and Adversarial Command & Control (AC2) Supremacy Matter

Regardless of who *owns* botnets, drones, and, swarms, those that *control* such botnets, drones, and, swarms shall determine global national security and homeland defense outcomes. Hence, there is a critical *pragmatic need* for developing U.S. national Command and Control Supremacy beyond "AI Supremacy" and "Quantum Supremacy." In fact, despite integration of latest and greatest advanced technologies such as AI and Quantum computing-based technologies, it is the weakest network link that can result in loss of C2 of the whole network as well as inter-network networks. Many of the latest and yet to be tested and validated technologies such as AI and Quantum Computing may result in the yet to be thoroughly stress-tested weakest links in the national and global Systems, Infrastructures, and, Networks. Hence, incorporation and integration of such technologies, particularly in relatively untested domains such as Air-Space-Cyberspace, may pose adversarial risks of appropriation of Command and Control of respective technologies and associated Systems, Infrastructures, and, Networks.

C4I-Cyber™ AFRL CA Venture: US C4I-Cyber Command and Control Supremacy: Adversarial Command and Control and Counter-Adversarial Command and Control

Advancing on 28-years of leading global Digital Transformation and associated Finance, IT, and, Cyber Risk Management practices, Global Risk Management Network, LLC[49] is currently leading the development of US C2 Supremacy & AC2 Supremacy Development. We are doing so through our AFRL Commercialization Academy Ventures AIMLExchange™ (AIMLExchange.com), BRINT® (BRINT.com), and C4I-Cyber™ (C4I-Cyber.com). Consistent with the track record of growing, building, and, leading Digital Transformation from its inception as global Digital pioneer starting with the beta version of the first Web browser,

we build related global Networks, Practices, Teams, Technologies, and, Ventures enabled by global virtual 'communities of practice' (CoPs). For example, C4I-Cyber™ is building a global CoP to enable US C2 Supremacy & AC2 Supremacy. Being situated proximal to the hub of the U.S. national leadership in C4I-Cyber, the AFRL and AFRL Commercialization Academy[50], our above ventures are members of the recent AFRL-CA cohorts. By developing a NYS community collaborative built upon the AFRL-CA tech ecosystem spanning the New York State, USA and the World, our ventures have already jumpstarted the above process. Using our social networks enterprises, we plan to also contribute to the local workforce development and economic development needs to enable the self-sustainment of the above NYS tech ecosystem.

C4I-Cyber™ C2:AC2:CAC2™ : Building NYS Tech Ecosystem for US C2:AC2:CAC2™ Supremacy Development

By developing a focused perspective beyond specific information technologies [which are a 'means' to an 'end' and not an 'end' in themselves], C4I-Cyber™ advances global practices in the pursuit of specific 'outcomes' that really matter regardless of enabling ITs. *What could be more critical than being able to sustain one's own 'command and control' given that if one loses that, one can lose ones "very existence"?* Hence, C4I-Cyber™ focuses on ensuring the viability of the "very existence" of associated Systems, Infrastructures, and, Networks to ensure the sustainability and survival of our nation and its society and enterprises. Our mission is aligned with the focus on "business continuity" focus of IT security given the historically unprecedented adversarial environments amidst exponentially growing vulnerabilities and exposures from integration of new technologies across new and unfamiliar domains. Following our applied R&D and practice methodologies used for world's largest firms and governments to tech startups, during recent years, we have been conducting 'gaps analysis' for our Network 'client' organizations including specific members C2 Networks. The 'gaps analysis' focuses on building 'capabilities' to serve 'needs' customized to known 'contributions' of such members toward development of cohesive global-national C2, AC2, & AC2 Supremacy Development[51].

I had the opportunity of invited interviews by the lead recruitment organization, Korn Ferry, for the US Air Force (USAF) Top Science Role of the USAF Chief Scientist, advisory role to the USAF Secretary and the Chiefs of USAF and US Space Force, while serving as the Chief Scientist on the Pentagon USAF C4I-ISR CTO-DoD CIO Senior Advisor Team[52]. That event had inspired such 'gaps analyses' for the Pentagon Joint Chiefs Advanced Battle Management System-Joint All Domain Command and Control (ABMS-JADC2). We thus advanced DoD leadership perspective beyond the diminishing efficacy of the Lethality Doctrine to the post-WWW realities of the Global C4I-Cyber-Crypto era of AI-Quantum technologies wherein C4I-Cyber Supremacy is often the most essential pre-requisite for AI and Quantum Supremacy. Our presentations and keynotes have advanced the Pentagon Joint Chiefs ABMS-JADC2 'Control Doctrine' focus to the next-generation 'cheaper, better, faster' ABMS2-JADAC2-JADCAC2 in the course of the New York State Governor's Cybersecurity presentations[53] and Quantum Engineering-PhD-Women Scientists 'Space for Women' Conference moderated by the USAF Modeling & Simulation CTO leader[54,55,56]. These are some representative examples of building New York State, US, and Global Networks, Practices, Teams, Technologies, and Ventures.

C4I-Cyber™ C2:AC2:CAC2™ : C2, AC2, & CAC2 and How They are Critical for Our Survival & Sustainability

- *Command & Control (C2)*: C2 is critical for survival and sustainability of respective enterprises. Regardless of whichever of above technologies are used, given that use of most of these 'advanced technologies' exponentially increases the vulnerability exposures and attack surfaces, mitigating the risk of loss of C&C is critical for survival and sustainability of all networked systems, enterprises, and, infrastructures.

- *Adversarial Command & Control (AC2)*: AC2 is the capability to stress test own products, services, and, infrastructures using advanced penetration testing and other techniques (such as for zero-day attacks) to ensure specific products, services, and, infrastructures demonstrate 'business continuity' of respective expected performance.

- Counter *Adversarial Command & Control (CAC2)*: CAC2 is the capability of countering the attacks from the adversaries that are exponentially increasing and threatening all networked systems, enterprises, and, infrastructures with increasingly greater vulnerability resulting from the integration of advanced technologies such as above and more so with the increasing integration of IoT and Block Chain technologies.

AIMLExchange™: Building NYS Tech Ecosystem for US C2:AC2:CAC2™ Supremacy Testing for AI-Quantum

AIMLExchange™ (AIMLExchange.com) is the 2019 New York State IDEA Awards Finalist, our AFRL Commercialization Academy venture saving digital CEO-CxO teams up to 90% time, cost, and, labor in execution. It does so by accelerating performance and minimizing risk in Knowing-Building-Monetizing™ global Digital, AI, ML, Quant, Cyber, Crypto and Quantum Practices, Technologies, Teams & Ventures[57,58]. Given exponentially increasing vulnerabilities with integration of advanced technologies in applied contexts and domains of application, AIMLExchange™ was inspired by the specific mission to 'Do Something Epic: Save the World™.[59] "We live in perilous times: applying incredibly powerful AI technologies across military and industry. With great power comes great responsibility. Such responsibility is all the more important given recent Weapon System Cybersecurity reports by the Pentagon and the GAO. These reports highlight a great paradox. The same AI technologies that enable military's automation and connectivity make the systems more vulnerable to cyber-attacks. 'Adversaries' can thus capture AI's 'control' to cause a global nuclear meltdown even when we 'own' the drones that command and control nuclear capabilities."

AIMLExchange™, by advancing upon our world-leading practices in IT, Risk Management, and, Risk Engineering, provides a readily usable template for global Digital teams adopting and implementing Digital, AI, ML, Quant, Cyber, Crypto and Quantum Technologies. In addition to encapsulating our guidance that has led hundreds of prior Digital teams deploying advanced technologies over prior 28-years, it also represents the complementary global CoP to C4I-Cyber™ for the development and deployment of AI, ML, Quant, Cyber, Crypto and Quantum Technologies. In addition, for the Pentagon Joint Chiefs ABMS-JADC2 subsequent evolution to ABMS2-JADAC2-JADCAC2, the above mentioned 'gaps analysis' with focus on building 'capabilities' driven by strategy and policy 'needs' has included the relevant focus on specific technologies that both enable C4I-Cyber and just like any other technology, are associated with causes of known and yet unknown 'zero day' vulnerabilities to consider.

AIMLExchange™: Digital, AI, ML, Quant, Cyber, Crypto and Quantum Practices, Technologies, & Ventures

The Knowledge Map accessible from the Top Menu of AIMLExchange.com captures our 28-year global Digital practices leadership with focus on Risk and Uncertainty Management characterizing the Future. Having led, and, guided hundreds of CEO-CxO Digital hi-tech teams including 1,000 MIT Management & Leadership industry executives on building global Practices, Technologies, and, Ventures, we developed the Know-Build-Monetize™ methodology to save CEOs-CxOs up to 90% Cost, Time, and, Resources in such executions. To enable thousands of global CEO-CxO digital teams at scale, AIMLExchange™ is building out Know-Build-Monetize™ methodology as a Global Digital Network Market Platform at AIMLExchange.com that anyone can access from diverse platforms including mobile devices. A perspective of the global reach and range of our global Digital Transformation CoP networks of practice is evident in having serviced millions of worldwide users. Another perspective is evident in having built a global collaborative community of over 130,000 to build our global Digital Practices in addition to a global virtual team of over 200 PhD industry experts. A complementary perspective of global impact is evident in the small sample of worldwide organizational clients, patrons, and users spanning most countries of the world listed below[60].

Global Corporations: Goldman Sachs, Google, HP, IBM, Intel, Microsoft, Wells Fargo
Consulting Firms: Accenture, Ernst & Young, McKinsey, PriceWaterhouseCoopers (PWC)
Healthcare: WHO, US Health & Human Services, UK Dept. of Health, European HMA
World Governments: Australia, Brazil, Canada, China, European Union, UK, USA
U.S. Defense: AFRL, Air Force, Army, CCRP, Comptroller, DISA, DoD, NASA, Navy
World Defense: Australia (Air Force), Canada (Defence R&D), UK (Ministry of Defence)
Universities: Harvard, INSEAD, MIT, Princeton, Stanford, UC Berkeley, Wharton
Associations: AACSB, ABA, ACM, AICPA, AOM, ASTD, ISACA, IEEE, INFORMS

Worldwide top leadership programs such as the Harvard MBA, world leaders such as Microsoft founder Bill Gates, Big-4 CxOs, and, CIOs of the US Army, US Navy, and US Air Force, and, the U.S. Joint Chiefs of Staff of the Department of Defense including U.S. National Heads of C4 Systems and National Defense University have adopted, applied, and recommended our Digital ventures transforming global digital practices. Worldwide Business and IT media have published unsolicited editorial reviews and invited interviews featuring them as global industrial benchmarks such as in Wall Street Journal, New York Times, Fortune, Fast Company, Forbes, Business Week, CIO, CIO Insight, Computerworld, Information Week, etc.

We Look Forward to Collaborating with You and others in enabling USA as Global Leader in Data Protection

Thank you for sharing your vision of the U.S. Data Protection Act and the Data Protection Agency in your article "The U.S. Needs a Data Protection Agency."[61] I am excited about your proposal having founded the world's largest Digital Transformation network of practice guiding worldwide Digital practices for U.S. and global firms and governments since over 28-years ago[62]. In the current proposal document, we provided actionable and specific execution advice and recommendations for the execution of the U.S. Data Protection Act for the Data Protection Agency to help enable the USA to lead Data Protection. We included actionable recommendations to enable USA to lead Data Protection by advancing *ex-ante* and *proactive* Data Protection to complement the current legal regulatory compliance framework. Additionally, we presented a reader-friendly overview of Network and Computer Security

Engineering issues material to legal and regulatory agencies for furthering their missions of the U.S. Data Protection Act. For execution and implementation of the proposal, we introduced the New York State tech ecosystem of the United States Air Force Research Lab (AFRL) and our associated Air Force Research Lab Commercialization Academy ventures. The AFRL-CA tech ecosystem and the ventures founded by our New York State venture capital firm, Global Risk Management Network, LLC, are pioneers and leaders of related global R&D and applied industrial practices in Data Protection. With IT Security, Risk Engineering, and, Risk Management leadership practices spanning critical national and global information infrastructures and Banking & Finance, Computer Software, Defense & Space, Government, Healthcare, Information Technology Services, Internet, and, Network & Computer Security industries among others, the AFRL-CA tech ecosystem and its practice leaders are ready to assist you in advancing the USA as a leader in Data Protection. We look forward to collaborating with you and others in your mission.

The current proposal document is also available online from my home page at:

https://www.yogeshmalhotra.com/DataProtectionAct.pdf .

REFERENCES:

AI-ML-QUANT-CYBER-CRYPTO-QUANTUM-RISK-COMPUTING-SOCIAL NETWORKS R&D PROGRAM

SSRN: 99 Top-10 R&D Rankings, Top 1% Author Ranking, 13,055 Downloads (as of 01/09/2023): R&D Impact among Artificial Intelligence-Quantitative Finance Nobel Laureates, AACSB-ASIS&T: CNet Networks Corporate Computing Award: Most Influential R&D: Why AI-KM Networks Fail. Listed papers are accessible for full-text download at Author's SSRN & Publications pages.
SSRN Author Page: 13,055 Downloads: https://papers.ssrn.com/author_id=2338267.
Google Scholar:10,000 Citations: https://scholar.google.com/citations?hl=en&user=MGblsfkAAAAJ .
Author Publications List: https://yogeshmalhotra.com/publications.html.

First Global Digital Transformation & AI-Quant-Cyber-Crypto-Quantum Risk Computing Networks:
www.YogeshMalhotra.com : We Create the Digital Future™. You Can Too! Let's Show You How!
AIMLExchange™: www.AIMLExchange.com : We Create the Digital Future™
BRINT™: www.BRINT.com : From Future of Finance™ to Future of FinTech™
C4I-Cyber™: www.C4I-Cyber.com : Because the Future of the World Depends Upon It™.

First Post-Doctoral Thesis: Quantitative Finance-Computer Science-Networks Security Engineering
Malhotra, Yogesh, A Report on the Future of Finance, Future of Risk, and Future of Quant: Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance and Advanced Analytics (January 19, 2015). A Report on the Future of Finance, Future of Risk, and Future of Quant: Risk, Uncertainty, and, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models using Quantitative Finance and Advanced Analytics. Abridged version: National Association of Insurance Commissioners (NAIC) Exp, Available at SSRN: https://ssrn.com/abstract=2553547 or http://dx.doi.org/10.2139/ssrn.2553547.

First PhD Thesis on Digital Social Networks, Risk Management and Control Models.
Malhotra, Y., *Role of Social Influence, Self-Determination and Quality of Use In Information Technology Acceptance And Utilization: A Theoretical Framework And Empirical Field Study*, PhD Thesis. University of Pittsburgh, Doctor of Philosophy Program, Joseph M. Katz Graduate School of Business, Pittsburgh: PA, July 1998, 181 pages, 120 Tables of Quantitative Analysis.

First Global Digital Transformation Network: Virtual Organization Pioneer Interviews.
Malhotra, Yogesh, (Interview). "On Becoming Virtual" (1997), *Training and Development*, American Society for Training and Development 55 (4): 30-37.
https://brint.org/AmericanSocietyforTrainingandDevelopmentInterview.pdf .

First Book on Global Knowledge Management & Virtual Organizations Practices
Malhotra, Yogesh, ed. *Knowledge management and virtual organizations*. IGI global, 2000.
https://www.amazon.com/stores/Yogesh-Malhotra/author/B001K80G96

First Book on Global Knowledge Management & Digital Business Models Innovation Practices
Malhotra, Yogesh, ed. *Knowledge Management and Business Model Innovation*. IGI global, 2001.
https://www.amazon.com/stores/Yogesh-Malhotra/author/B001K80G96

First CRM Paper on Self-Determination of Users in Digital Social Networks.
Malhotra, Yogesh, "Desperately Seeking Self-Determination: Key to the New Enterprise Logic of Customer Relationships" (2004). AMCIS 2004 Proceedings. 490.
https://aisel.aisnet.org/amcis2004/490 .

Malhotra, Yogesh, Cybersecurity & Cyber-Finance Risk Management: Strategies, Tactics, Operations, &, Intelligence: Enterprise Risk Management to Model Risk Management: Understanding Vulnerabilities, Threats, & Risk Mitigation (Presentation Slides) (September 15, 2015). Available at SSRN: https://ssrn.com/abstract=2693886 or http://dx.doi.org/10.2139/ssrn.2693886 .

Malhotra, Yogesh, AI, Machine Learning & Deep Learning Risk Management & Controls: Beyond Deep Learning and Generative Adversarial Networks: Model Risk Management in AI, Machine Learning & Deep Learning: Princeton Presentations in AI-ML Risk Management & Control Systems (Presentation Slides) (April 21, 2018). Princeton Presentations in AI & Machine Learning Risk Management & Control Systems, 2018 Princeton Fintech & Quant Conference, Princeton University, April 21, 2018., Available at
SSRN: https://ssrn.com/abstract=3167035 or http://dx.doi.org/10.2139/ssrn.3167035.

Malhotra, Yogesh, Beyond Model Risk Management to Model Risk Arbitrage for FinTech Era: How to Navigate 'Uncertainty'...When 'Models' Are 'Wrong'...And Knowledge'...'Imperfect'! Knight Reconsidered Again: Risk, Uncertainty, & Profit Beyond ZIRP & NIRP (April 16, 2016). Research Presentation at: 2016 Princeton Quant Trading Conference, Princeton University, Available at
SSRN: https://ssrn.com/abstract=2766099 or http://dx.doi.org/10.2139/ssrn.2766099.

Malhotra, Yogesh, Cognitive-Neuromorphic Computing for Anticipatory Risk Analytics in Intelligence, Surveillance & Reconnaissance (ISR): Model Risk Management in Artificial Intelligence & Machine Learning (Presentation Slides) (January 28, 2018). Available at
SSRN: https://ssrn.com/abstract=3111837 or http://dx.doi.org/10.2139/ssrn.3111837.

Malhotra, Yogesh, AI, Machine Learning & Deep Learning Risk Management & Controls: Beyond Deep Learning and Generative Adversarial Networks: Model Risk Management in AI, Machine Learning & Deep Learning (May 16, 2018). Paper Accepted for Presentation at the 2018 Armed Forces Communications and Electronics Association (AFCEA) C4I and Cyber Conference, Erie Canal Chapter, New York, June 19 & 20, 2018. , Available at
SSRN: https://ssrn.com/abstract=3193693 or http://dx.doi.org/10.2139/ssrn.3193693.

Malhotra, Yogesh, JP Morgan Funds of Funds Alternative Assets Portfolio Optimization With VaR, ES, CVAR, ARCH/GARCH and EVT Stress Testing: Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management: How to Manage Risk (After Risk Management Has Failed) for Hedge Funds (December 4, 2014). Available at
SSRN: https://ssrn.com/abstract=2538401 or http://dx.doi.org/10.2139/ssrn.2538401.

Malhotra, Yogesh, CreditMetrics Methodology and Credit Value at Risk (Credit VaR) (February 10, 2021). Available at
SSRN: https://ssrn.com/abstract=3783490 or http://dx.doi.org/10.2139/ssrn.3783490.

Malhotra, Yogesh, Markov Chain Monte Carlo Models, Gibbs Sampling, & Metropolis Algorithm for High-Dimensionality Complex Stochastic Problems (May 8, 2014). Available at
SSRN: https://ssrn.com/abstract=2553537 or http://dx.doi.org/10.2139/ssrn.2553537.

Malhotra, Yogesh, Power Point Presentation: AI-Machine Learning Augmentation and Cybersecurity: Why Smart Minds Using Smart Tools Are Critical for Minimizing Risks, And, What You Can Do About It? (June 4, 2019). Presentation: 2019 New York State Cyber Security Conference, Albany, NY, June 4 - 5, 2019, Empire State Plaza , Albany, NY, Available at
SSRN: https://ssrn.com/abstract=3399781 or http://dx.doi.org/10.2139/ssrn.3399781.

Malhotra, Yogesh, Bitcoin Protocol: Model of 'Cryptographic Proof' Based Global Crypto-Currency & Electronic Payments System (December 4, 2013). Available at SSRN: https://ssrn.com/abstract=2911623 or http://dx.doi.org/10.2139/ssrn.2911623.

Malhotra, Yogesh, Future of Finance Beyond 'Flash Boys': Risk Modeling for Managing Uncertainty in an Increasingly Non-Deterministic Cyber World: Knight Reconsidered: Risk, Uncertainty, and Profit for the Cyber Era (Presentation Slides) (April 4, 2015). Princeton Quant Trading Conference 2015, Available at SSRN: https://ssrn.com/abstract=2590258 or http://dx.doi.org/10.2139/ssrn.2590258.

Malhotra, Yogesh, A Risk Management Framework for Penetration Testing of Global Banking & Finance Networks VoIP Protocols (May 8, 2014). Available at SSRN: https://ssrn.com/abstract=2555098 or http://dx.doi.org/10.2139/ssrn.2555098.

Malhotra, Yogesh, Advancing Cyber Risk Insurance Underwriting Model Risk Management beyond VaR to Pre-Empt and Prevent the Forthcoming Global Cyber Insurance Crisis (December 7, 2017). Available at SSRN: https://ssrn.com/abstract=3081492 or http://dx.doi.org/10.2139/ssrn.3081492.

Malhotra, Yogesh, Measuring & Managing Financial Risks with Improved Alternatives Beyond Value-at-Risk (VaR) (January 26, 2012). Available at SSRN: https://ssrn.com/abstract=2594859 or http://dx.doi.org/10.2139/ssrn.2594859.

Malhotra, Yogesh, Quantitative Modeling of Trust and Trust Management Protocols in Next-Generation Social Networks-Based Wireless Mobile AD HOC Networks (April 1, 2017). IUP Journal of Computer Sciences, Vol. XI, No. 2, pp. 7-28. April 2017, Available at SSRN: https://ssrn.com/abstract=2983573.

Malhotra, Yogesh, CyberFinance: Why Cybersecurity Risk Analytics Must Evolve to Survive 90% of Emerging Cyber Financial Threats, and, What You Can Do About It? Advancing Beyond 'Predictive' to 'Anticipatory' Risk Analytics (June 8, 2016). Research Presentation at the 19th New York State Cyber Security Conference Presentation, Albany, NY, June 8-9, 2016, Empire State Plaza, Albany, NY., Available at SSRN: https://ssrn.com/abstract=2791863 or http://dx.doi.org/10.2139/ssrn.2791863.

Malhotra, Yogesh, The CFA Society Keynote: Advancing Hedge Funds Chief Investment Officer Practices: Model Risk Management with Auto Machine Learning: JP Morgan and Goldman Sachs Practices Case Studies. (Presentation: 107 slides) (October 16, 2018). Available at SSRN: https://ssrn.com/abstract=3312568 or http://dx.doi.org/10.2139/ssrn.3312568.

Malhotra, Yogesh, Why Encryption and Crypto Systems Fail and How to Preempt and Prevent Such Systems Failures: Cryptology beyond Shannon's Information Theory: Preparing for When the 'Enemy Knows the System': Technical Focus on Number Field Sieve Cryptanalysis Algorithms for Most Efficient Prime Factorization on Composites (January 9, 2019). Available at SSRN: https://ssrn.com/abstract=2553544 or http://dx.doi.org/10.2139/ssrn.2553544.

Malhotra, Yogesh, Toward Integrated Enterprise Risk Management, Model Risk Management & Cyber-Finance Risk Management: Bridging Networks, Systems and Controls Frameworks (October 22, 2015). Presented at: 2015 NY Cyber Security & Engineering Technology Association Conference, Oct. 22, 2015, Rochester Institute of Technology, Rosica Hall, NTID, Rochester, New York, Available at SSRN: https://ssrn.com/abstract=2792629 or http://dx.doi.org/10.2139/ssrn.2792629.

Malhotra, Yogesh, How You Can Implement Well-Architected 'Zero Trust' Hybrid-Cloud Computing Beyond 'Lift and Shift': Cloud-Enabled Digital Innovation at Scale with Infrastructure as Code (IaC), DevSecOps and MLops (June 8, 2022). 2022 New York State Cyber Security Conference: Invited

Presentations, Albany, New York: https://its.ny.gov/2022-nyscsc, Available at SSRN: https://ssrn.com/abstract=4131044 or http://dx.doi.org/10.2139/ssrn.4131044.

Malhotra, Yogesh, Communications: Making Quantum Computing Real for JADC2 With Qiskit: Quantum Enabling Technologies for Applications to Support Communication and Networking: White Paper Submitted for the Global Competition: AFRL Innovare Million Dollar International Quantum U Tech Accelerator (August 4, 2020). Available at SSRN: https://ssrn.com/abstract=3682216 or http://dx.doi.org/10.2139/ssrn.3682216.

Malhotra, Yogesh, Guidance to a Goldman Sachs alumnus Hedge Fund with $400 Billion-$500 Billion AUM: Alpha Trading Strategies Analysis, Maximizing Alpha for Hedge Funds, and, High Frequency Econometrics for Analyzing Price Impact of Trades, Liquidity, and, Market Microstructure (December 26, 2018). Available at SSRN: https://ssrn.com/abstract=3306817 or http://dx.doi.org/10.2139/ssrn.3306817.

Malhotra, Yogesh, Advancing Cognitive Analytics Using Quantum Computing for Next Generation Encryption (Presentation Slides) (March 24, 2017). Available at SSRN: https://ssrn.com/abstract=2940467 or http://dx.doi.org/10.2139/ssrn.2940467.

Malhotra, Yogesh, Beyond Data Protection to Command and Control (C2) Sustainability in a Post-COVID19 World: Execution of U.S. Data Protection Act for U.S. Data Protection Agency (April 21, 2020). Available at SSRN: https://ssrn.com/abstract=3581454 or http://dx.doi.org/10.2139/ssrn.3581454.

Malhotra, Yogesh, Bridging Networks, Systems and Controls Frameworks for Cybersecurity Curricula & Standards Development (October 22, 2015). 2015 NY Cyber Security & Engineering Technology Association Conference, Oct. 22, 2015 Rochester Institute of Technology, Rosica Hall, NTID, Rochester, New York, Available at SSRN: https://ssrn.com/abstract=2792636 or http://dx.doi.org/10.2139/ssrn.2792636.

Malhotra, Yogesh, C++11 for Hedge Fund Traders and Investment Bankers: Concurrency and Multithreading With C++11 for Thread Management & Data Sharing Between Threads (Presentation Slides) (June 18, 2019). Available at SSRN: https://ssrn.com/abstract=3406364 or http://dx.doi.org/10.2139/ssrn.3406364.

Malhotra, Yogesh, C4I-Cyber Command & Control Supremacy: Why It's More Critical Than AI & Quantum Supremacy & What You Can Do about It? Security in Post-COVID Virtual Era Beyond Data, Models, Algorithms (May 24, 2021). Forthcoming, 2021 New York State Cyber Security Conference, June 8-9, 2021, Empire State Plaza - Albany, NY., Available at SSRN: https://ssrn.com/abstract=3851807 or http://dx.doi.org/10.2139/ssrn.3851807.

Malhotra, Yogesh, If You Build It, They Will Come: Getting U.S. Vocational Colleges to Deliver 'Job Ready' Graduates for 'Real Jobs' of the 'Real World' (Presentation Slides) (March 22, 2018). Available at SSRN: https://ssrn.com/abstract=3147046 or http://dx.doi.org/10.2139/ssrn.3147046.

Malhotra, Yogesh, Global Finance Liquidity Risk Revisited: JP Morgan Alternative Assets Portfolio Liquidity Assessment Framework & Models: $500 Billion Fund of Funds: 17 Asset Classes (June 14, 2022). Available at SSRN: https://ssrn.com/abstract=4135904 or http://dx.doi.org/10.2139/ssrn.4135904.

Malhotra, Yogesh, Global Finance Liquidity Risk Revisited: Development of a Framework for Liquidity Assessment in Portfolio Construction Process: Presentations to the JP Morgan Global Head of Quant

Research & Analytics and Us Head of Portfolio Construction Teams (July 23, 2022). JP Morgan Quantitative Finance Risk Modeling Presentations to JP Morgan Global Head of Quant Research & Analytics-JP Morgan US Head of Portfolio Construction Executive Director and Quantitative-Financial Engineers-Developers Team (2022), Available at SSRN: https://ssrn.com/abstract=4170996.

Malhotra, Yogesh, Catastrophic Risk Modeling for Risk Strategy Execution: Extreme Risk Models and Methods: Cyber Finance to Cyber Warfare Risk Modeling for Managing Exponential Uncertainty and Complexity in Increasingly Non-Deterministic Cyberspace (August 2015). State Street, 2015, Available at SSRN: https://ssrn.com/abstract=3780163.

Malhotra, Yogesh, Anticipatory Risk Analytics for Global Response on the Containment of COVID-19 (March 17, 2020). Available at SSRN: https://ssrn.com/abstract=3682207 or http://dx.doi.org/10.2139/ssrn.3682207.

Malhotra, Yogesh, Advancing Beyond IT Management Failures to Knowledge Management: Foundations of Knowledge-Based Enterprises and Knowledge Work: Invited Presentation at The Monieson Centre for Knowledge-Based Enterprises Queen's School of Business: Queen's University Kingston, Ontario, Canada (Presentation Slides) (March 24, 2006). Available at SSRN: https://ssrn.com/abstract=3340097 or http://dx.doi.org/10.2139/ssrn.3340097.

Malhotra, Yogesh, VigiTrust Global Advisory Board Keynote: How to Manage Geopolitical Crisis-Risks: Protecting Global & National Critical Infrastructures (Presentation Slides) (March 30, 2022). March 30, 2022: VigiTrust Global Advisory Board Keynote, How to Manage Geopolitical Crisis-Risks: Protecting Global & National Critical Infrastructures, Dr. Yogesh Malhotra: Keynote Video Presentation: https://youtu.be/jor6lojSJmM [Slide Deck]., Available at SSRN: https://ssrn.com/abstract=4071293.

Malhotra, Yogesh, Beyond 'Bayesian vs. Var' Dilemma to Empirical Model Risk Management: Managing Risk for Hedge Funds (December 12, 2022). Malhotra, Yogesh, Beyond 'Bayesian vs. VaR' Dilemma to Empirical Model Risk Management: Managing Risk for Hedge Funds. The IUP Journal of Financial Risk Management, Vol. 19, No. 2, 2022, Available at SSRN: https://ssrn.com/abstract=4301788.

Malhotra, Yogesh, Framework of CreditMetrics Methodology for Credit VaR (December 14, 2022). Malhotra, Yogesh, Framework of CreditMetrics Methodology for Credit VaR. The IUP Journal of Financial Risk Management, Vol. 19, No. 3, 2022., Available at SSRN: https://ssrn.com/abstract=4301859.

Malhotra, Yogesh, Bridging Networks, Systems and Controls Frameworks for Cybersecurity Curriculums and Standards Development (March 26, 2018). Journal of Operational Risk, Vol. 13, No. 1, 2018, Available at SSRN: https://ssrn.com/abstract=3149414.

Malhotra, Yogesh, Artificial Intelligence Augmentation for Large-Scale Global Systemic and Cyber Risk Management Projects: Model Risk Management for Minimizing the Downside Risks of Artificial Intelligence and Machine Learning (April 29, 2019). Journal of Financial Transformation, Capco Institute (UK), Vol. 49, pp. 94-99. April 2019, Available at SSRN: https://ssrn.com/abstract=4076445.

Malhotra, Yogesh, US Air Force–Space Force: Beyond ABMS-JADC2 to Faster-Better-Cheaper ABMS2 JADAC2-JADCAC2: AI-Quantum Cyber-Crypto-EMS Network-Centric Computing with Autonomous Robots in Air & Space: Beyond the 'Quantum' Silo to Real-World 'AI-Cyber-Crypto-Quantum' (November 20, 2020). Available at SSRN: https://ssrn.com/abstract=3734680.

Malhotra, Yogesh, Bahamas e-Government: Single Digital ID for citizens of The Bahamas: Toward a National Cybersecurity System to Ensure Data Privacy and Security (July 1, 2018). Available at SSRN: https://ssrn.com/abstract=3739258.

Malhotra, Yogesh, Existing & Emerging Sectors of AI, Cybersecurity, Defense and Law Enforcement (January 26, 2022). ConnectAI 2022 Digital Masterclass: Video of Conference Presentation: https://www.youtube.com/watch?v=JGB76NJRRBU, Available at SSRN: https://ssrn.com/abstract=4018644.

Malhotra, Yogesh, Future of Bitcoin & Statistical Probabilistic Quantitative Methods: Global Financial Regulation (Interview: Hong Kong Institute of CPAs) (January 20, 2014). Global official magazine of the Hong Kong Institute of Certified Public Accountants, 2014, Available at SSRN: https://ssrn.com/abstract=2911645.

Malhotra, Yogesh, C4I-Cyber Command & Control Supremacy: Why It's More Critical Than AI & Quantum Supremacy & What You Can Do about It? Security in Post-COVID Virtual Era Beyond Data, Models, Algorithms (Interactive PowerPoint Slides To Accompany Virtual Conference Keynote) (June 5, 2021). Available at SSRN: https://ssrn.com/abstract=3860948.

Malhotra, Yogesh, How Has Artificial Intelligence Challenged the Boundaries of Humanistic Thinking? Global Conference on Artificial Intelligence and Machine Learning: The Future is Now: Data Bridge Market Research (October 13, 2021). Available at SSRN: https://ssrn.com/abstract=3941835.

Malhotra, Yogesh, Growing Digital Startups to Trillion $ Hedge Funds: Saving You 90% Time & Cost for Sustainable Resilience: Pioneering Global Digital Transformation from Silicon Valley to Wall Street to Pentagon since the beginning of the 'Wild Wild Web' (Presentation Slides) (January 19, 2021). Available at SSRN: https://ssrn.com/abstract=3769330.

Malhotra, Yogesh, Future of Risk is [Already] Quantum, Are You Prepared?: Journal of Knowledge Engineering & Management (Forthcoming), Pre-Print Abstract: Available at SSRN: https://ssrn.com/abstract=4209810

Malhotra, Yogesh, and Dennis F. Galletta. "Extending the technology acceptance model to account for social influence: Theoretical bases and empirical validation." *Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences. 1999. HICSS-32. Abstracts and CD-ROM of Full Papers*. IEEE, 1999.

Malhotra, Yogesh. "Why knowledge management systems fail: enablers and constraints of knowledge management in human enterprises." *Handbook on Knowledge Management 1*. Springer, Berlin, Heidelberg, 2004. 577-599.

Malhotra, Yogesh. "Integrating knowledge management technologies in organizational business processes: getting real time enterprises to deliver real business performance." *Journal of knowledge management* (2005).

Malhotra, Yogesh. "Knowledge management for e-business performance: advancing information strategy to "internet time"." *Information Strategy: The Executive's Journal* 16.4 (2000): 5-16.

Malhotra, Yogesh. "Knowledge Management for the New World of Business", Originally Titled: Tools@work: Deciphering the Knowledge Management Hype, *The Journal for Quality and Participation*; Cincinnati; Jul/Aug 1998, 21(4), 58-60. URL: https://www.brint.com/km/whatis.htm .

Malhotra, Yogesh. "Knowledge management and new organization forms: A framework for business model innovation." *Intelligent Support Systems: Knowledge Management*. IGI Global, 2002. 177-199.

Malhotra, Yogesh. "Knowledge assets in the global economy: assessment of national intellectual capital." *Intelligent support systems: Knowledge management*. IGI Global, 2002. 22-42.

Malhotra, Yogesh. "Measuring knowledge assets of a nation: knowledge systems for development." *Invited Research Paper Sponsored by the United Nations Department of Economic and Social Affairs. Keynote Presentation at the Ad Hoc Group of Experts Meeting at the United Nations Headquarters, New York City, NY*. 2003.

Malhotra, Yogesh, and Dennis Galletta. "A multidimensional commitment model of volitional systems adoption and usage behavior." *Journal of Management Information Systems* 22.1 (2005): 117-151.

Malhotra, Yogesh, "Knowledge Management in Inquiring Organizations" (1997). AMCIS 1997 Proceedings. 181. http://aisel.aisnet.org/amcis1997/181.

Malhotra, Yogesh. "Business Process Redesign: An Overview," *IEEE Engineering Management Review*, vol. 26, no. 3, Fall 1998.

Malhotra, Yogesh. "Knowledge management for e-business performance: advancing information strategy to "Internet Time"." *Making Supply Chain Management Work*. Auerbach Publications, 2001. 623-638.

Malhotra, Yogesh. "From information management to knowledge management: Beyond the" hi-tech hidebound" systems." *Knowledge management and business model innovation*. IGI Global, 2001. 115-134.

Malhotra, Yogesh, Dennis F. Galletta, and Laurie J. Kirsch. "How endogenous motivations influence user intentions: Beyond the dichotomy of extrinsic and intrinsic user motivations." *Journal of Management Information Systems* 25.1 (2008): 267-300.

Malhotra, Yogesh, and D. F. Galleta. "Role of commitment and motivation in knowledge management systems implementation: Theory, conceptualization, and measurement of antecedents of success." *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the*. IEEE, 2003.

Malhotra, Yogesh. (1996). Organizational Learning and Learning Organizations: An Overview [WWW document]. URL http://www.brint.com/papers/orglrng.htm .

King, William R., and Yogesh Malhotra. "Developing a framework for analyzing IS sourcing." *Information & management* 37.6 (2000): 323-334.

Malhotra, Yogesh, and Dennis F. Galletta. "Building systems that users want to use." *Communications of the ACM* 47.12 (2004): 88-94.

Malhotra, Yogesh. (1998). Knowledge Management, Knowledge Organizations & Knowledge Workers: A View from the Front Lines, Invited Interview by Maeil Business Newspaper, Korea. [WWW document]. URL: http://www.brint.com/interview/maeil.htm .

Malhotra, Yogesh. "Expert systems for knowledge management: crossing the chasm between information processing and sense making." *Expert Systems with Applications* 20.1 (2001): 7-16.

Malhotra, Yogesh, "Information Ecology and Knowledge Management: Toward Knowledge Ecology for Hypertubulent Organizational Environments" (2002). Management - All Scholarship. 3. https://surface.syr.edu/mgt/3 .

Malhotra, Yogesh. " Enabling Knowledge Exchanges for E-Business Communities." *Information Strategy.* 18.3 (2002): 26-31.

Malhotra, Yogesh. "Is knowledge management really an oxymoron? Unraveling the role of organizational controls in knowledge management." *Knowledge mapping and management*. IGI Global, 2002. 1-13.

Malhotra, Yogesh. "Organizational controls as enablers and constraints in successful knowledge management systems implementation." *Knowledge management and business model innovation*. IGI Global, 2001. 326-336.

Malhotra, Yogesh. "Controlling copyright infringements of intellectual property: the case of computer software-Part Two." *Journal of Systems Management* 45.7 (1994): 12-19.

Malhotra, Yogesh. "Bringing the adopter back into the adoption process: a personal construction framework of information technology adoption." *Journal of High Technology Management Research* 10.1 (1999): 79-104.

Malhotra, Yogesh. "Enabling Next Generation e-Business Architectures: Balancing Integration and Flexibility for Managing Business Transformation." Intel Corporation Expert Paper (2001).

Malhotra, Yogesh. "Role of Organizational Controls in Knowledge Management: Is Knowledge Management Really an “Oxymoron”. *Knowledge Management and Virtual Organizations* (2000): 245.

End Notes: Hyperlinks to all referenced articles as checked on January 8th, 2023.

[1] https://medium.com/@gillibrandny/the-u-s-needs-a-data-protection-agency-98a054f7b6bf
[2] https://FinRM.com/globalimpact.html
[3] https://shoshanazuboff.com/book/
[4] http://www.BRINT.org/km/KnowledgeManagementMeasurementResearch/technologyacceptance.pdf
[5] https://www.kmnetwork.com/ITUseCACM.pdf
[6] https://BRINT.org/NewLogicOfCRM.pdf
[7] https://www.BRINT.org/JMIS.pdf
[8] https://www.BRINT.org/JMIS2.pdf
[9] https://www.yogeshmalhotra.com/rankings.html
[10] https://FinRM.com/casestudies.html
[11] https://www.FinRM.com/Background.html
[12] https://www.fastcompany.com/39678/nerds-need-apply
[13] https://www.nytimes.com/2020/01/10/technology/facebook-election.html
[14] https://www.theatlantic.com/technology/archive/2017/10/what-facebook-did/542502/
[15] https://ssrn.com/abstract=3399781
[16] https://ssrn.com/abstract=2791863
[17] https://ssrn.com/abstract=4131044
[18] https://ssrn.com/abstract=3851807
[19] https://ssrn.com/abstract=2590258
[20] https://ssrn.com/abstract=2766099
[21] https://ssrn.com/abstract=3167035
[22] https://AIMLExchange.com/MIT/
[23] https://ssrn.com/abstract=2911623
[24] https://ssrn.com/abstract=2911645
[25] https://ssrn.com/abstract=3739258
[26] https://ssrn.com/abstract=4131044
[27] https://www.youtube.com/watch?v=1gd6mKeHJuw
[28] https://ssrn.com/abstract=3193693
[29] https://ssrn.com/abstract=3111837
[30] https://www.yogeshmalhotra.com/Cybersecurity.html
[31] https://www.youtube.com/watch?v=1gd6mKeHJuw
[32] https://ssrn.com/abstract=2553547
[33] https://ssrn.com/abstract=2693886
[34] https://www.cdc.gov/coronavirus/2019-ncov/about/transmission.html
[35] https://www.yogeshmalhotra.com/GriffissCyberspace.html
[36] https://www.risk.net/journal-of-operational-risk/5462036/bridging-networks-systems-and-controls-frameworks-for-cybersecurity-curriculums-and-standards-development
[37] https://ssrn.com/abstract=4209810
[38] https://news.sophos.com/en-us/2014/03/26/how-malware-works-anatomy-of-a-drive-by-download-web-attack-infographic/
[39] https://www.bloomberg.com/news/articles/2018-01-08/-it-can-t-be-true-inside-the-semiconductor-industry-s-meltdown
[40] https://ssrn.com/abstract=2553547
[41] https://www.cdc.gov/coronavirus/2019-ncov/about/transmission.html
[42] https://www.youtube.com/watch?v=1eu8QJRyDMQ
[43] https://www.theverge.com/2020/2/13/21135231/kirsten-gillibrand-facebook-google-data-protection-agency-privacy-big-tech
[44] https://ssrn.com/abstract=2766099
[45] https://ssrn.com/abstract=2553547
[46] https://www.risk.net/journal-of-operational-risk/5462036/bridging-networks-systems-and-controls-frameworks-for-cybersecurity-curriculums-and-standards-development
[47] https://yogeshmalhotra.com/Resume.pdf
[48] https://yogeshmalhotra.com/bio.html
[49] https://www.linkedin.com/company/global-risk-management-network-llc/

[50] https://griffissinstitute.org/who-we-work-with/afrl/tech-transfer/commercialization-academy
[51] https://www.youtube.com/@dr.yogeshmalhotrawecreatet396
[52] https://www.youtube.com/watch?v=XPV-AV17rk0
[53] https://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=2338267
[54] https://www.youtube.com/watch?v=cKEWHOPOhy0
[55] https://www.youtube.com/watch?v=Sbq3j6Jkvsw
[56] https://www.youtube.com/watch?v=2QBH2RcPURQ
[57] https://www.youtube.com/watch?v=XPV-AV17rk0
[58] https://www.youtube.com/watch?v=QzqIfJ32ycg
[59] https://AIMLExchange.com/aboutus.html#SavetheWorld
[60] https://www.yogeshmalhotra.com/globalimpact.html
[61] https://medium.com/@gillibrandny/the-u-s-needs-a-data-protection-agency-98a054f7b6bf
[62] https://FinRM.com/globalimpact.html