Joseph N. Pelton
Indu B. Singh

Smart Cities of Today and Tomorrow

Better Technology, Infrastructure and Security

Springer

Smart Cities of Today and Tomorrow

Joseph N. Pelton • Indu B. Singh

Smart Cities of Today and Tomorrow

Better Technology, Infrastructure and Security

Copernicus Books is a brand of Springer

Joseph N. Pelton
IAASS
Arlington, VA, USA

Indu B. Singh
Planet Defense, LLC
Fairfax, VA, USA

ISBN 978-3-319-95821-7 ISBN 978-3-319-95822-4 (eBook)
https://doi.org/10.1007/978-3-319-95822-4

Library of Congress Control Number: 2018951219

© Springer International Publishing AG, part of Springer Nature 2019
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

Preface

In 2008, both authors were heavily involved in urban planning. In one instance, Joe Pelton was chairing the IT Advisory Commission for Arlington County, Virginia, and also preparing a proposal nominating Arlington County for the Intelligent Community Award as annually presented by the Intelligent Community Forum. In the other instance, Indu Singh was then involved in advising communities on three continents about how to design smart communities responsive to citizen needs and also include the most appropriate new technology. We had also worked together over the years in closely related fields. That year, we had also decided to put on a conference on emergency communications at George Washington University, where one of us then headed a telecommunications and computer program. During our collaboration, we decided to write a book entitled *Future Cities* that was published in 2009. We followed that initiative by writing another book together entitled *Safe Cities: Living Free in a Dangerous World.* This was published by the Emerald Planet in 2013. Then, we next worked together on *Digital Defense: A Primer in Cyber Security* that we published in 2015.

This lasting and effective partnership has now continued, and this is our latest book. It explores the ins and outs of planning, designing, implementing, and operating an intelligent community. This book, *Smart Cities of Today and Tomorrow,* combines the experience and research represented by our two different yet interlinked lifetimes of practical consulting and academic experience. We have been involved in the planning and engineering of telecommunication and IT systems, of security networks, of urban infrastructure, and of city planning, and this book reflects the knowledge and research findings we have accumulated through this process. We believe in more effective and brighter urban futures and hope this book might help light the way.

Certainly one of the keys to good smart city planning is to engage the citizenry in effective and responsive ways to make their cities a better place to live. We hope what follows is a useful guide with regard to key issues and offers useful advice about better ways to involve citizenry in the planning process. Further, we hope it illuminates some smarter ways to make key urban investment and planning decisions and create better longer-term goals and a clear vision of what you want your city to become.

There are many things to consider in trying to plan and create a smart city, but if we were to try to boil down our top advice to a single sentence, it would be along these lines: suburban sprawl is bad, and thus urban density is good, but when a city becomes ultra-dense, this intense overconcentration of people, transport systems, and infrastructure becomes bad again. We believe scale and what we call meta-city planning concepts are keys to a smart city as much as the use of smart technology.

Arlington, VA, USA — Joseph N. Pelton
Fairfax, VA, USA — Indu B. Singh

Acknowledgments

This book has been in preparation for some time, and many people have assisted in the research, review of preliminary text, and suggestion of key topics to be included and analyzed. Those that we wish to express our appreciation to include John Bone and Michael Oehler of Planet Defense LLC. A number of governmental officials of Arlington County such as Jack Belcher and Robert Duffy as well as County Board Member Christian Dorsey have offered useful information concerning planning practices in Arlington County, Virginia. Further I would like to thank those with special knowledge of the field who have also offered advice and counsel such as Frank Jazzo, Martha Moore, Philip Caughran, Barbara Allen, and Alexander Pelton. Advisors, we also extend our thanks. At Springer Press, Maury Solomon and Hannah Kaufman, as always, have been kind, thoughtful, and quite helpful in their support. Finally, Peter Marshall, my friend and colleague, has provided skill and special insight in his masterful editing skills. As always, we are responsible for the accuracy of all the contents of this book, but we do greatly appreciate the support we have received.

Contents

About the Authors

Joseph N. Pelton is a widely published award-winning author with some 50 books written, coauthored, edited, or coedited. His *Global Talk* won the Eugene Emme Literature Award and was nominated for a Pulitzer Prize. He is the coauthor with Dr. Singh of the book *Future Cities* published by the Intelligent Communities Forum in 2009 and *The Safe City: Living Free in a Dangerous World* in 2013. Dr. Pelton is currently the principal of Pelton Consulting International. He is on the executive board of the International Association for the Advancement of Space Safety and chair of its International Academic Advisory Committee as well as the former president of the International Space Safety Foundation. He is the former dean of the International Space University (ISU) of Strasburg, France. He also served as chairman of the ISU's Board of Trustees. He is the director emeritus of the Space and Advanced Communications Research Institute (SACRI) at George Washington University. Dr. Pelton was the director of the Interdisciplinary Telecommunications Program at the University of Colorado from 1988 to 1997. At the time, it was the largest such graduate program in the United States. During his academic career, Professor Pelton taught at American University, the University of Colorado Boulder, and George Washington University and served as VP of academic affairs at the ISU. His undergraduate degree in physics is from the University of Tulsa, his master's is from New York University, and his PhD is from Georgetown University in political science and international relations. He previously held various executive positions at Intelsat and Comsat, including serving as

director of Project SHARE and director of strategic policy for Intelsat. Intelsat's Project SHARE gave birth to the Chinese National TV University and many other tele-health and tele-education programs around the world. Dr. Pelton was the founder of the Arthur C. Clarke Foundation and served for many years as its executive director. He was also the founding president of the Society of Satellite Professionals (SSPI) and has been recognized in the SSPI Hall of Fame. He has served on the Board of the International Institute of Communications. He has been active with the World Future Society and also frequently speaks and writes as a futurist. Dr. Pelton is a member of the International Academy of Astronautics, an associate fellow of the American Institute of Aeronautics and Astronautics (AIAA), and a fellow of the International Association for the Advancement of Space Safety (IAASS). He is the winner of the IAASS da Vinci Award and the 2017 Guardian Award of the Life Boat Foundation, which has been previously won by Bill Gates, Elon Musk, Warren Buffet, and Prince Charles. He has served as president of the Arlington County Civic Federation, as a member of its Long-Range County Improvement Commission that initiated "smart growth" in Arlington, and as also the immediate past chair of the IT Advisory Commission for Arlington County that plays a key role in protecting the safety and resilience of the county's telecommunications and IT networks and helps to initiate the ConnectArlington fiber optic network. Dr. Pelton resides in Arlington County, Virginia.

Indu B. Singh, Ph.D. is president and CEO of Planet Defense LLC. He is an internationally recognized consultant for smart cities and cybersecurity. Most recently, he served as senior director in the Intelligence Services Division of General Dynamic Information Technology (GDIT). Prior to this, Dr. Singh was vice president and head of Washington, DC, operations for Los Alamos Technical Associates (LATA). Dr. Singh also served as executive director of LATA's Global Institute for Security and Training (GIST), which he founded in 2012. Prior to joining LATA, Dr. Singh served as director and managing partner in Federal Government Services at Deloitte Consulting LLC, where he managed systems engineering and security practice. At BearingPoint, Inc. (formerly KPMG Consulting), Dr. Singh was a managing director

and partner and operated his global practice in systems engineering, security, and IT transformation. Dr. Singh is considered a pioneer in the designing and implementing of smart cities and safe cities around the world. He has led projects to design, build, and completely implement new cities and urban security and IT systems in the United States, Europe, Asia, and the Middle East. Dr. Singh has led workshops and seminars in a number of areas such as urban security systems, cyber defense for smart cities, designing and building of smart cities, as well advance training in cybersecurity and the smart city. He has significant business and technology management experience with a proven P&L track record. Dr. Singh founded three midsize high-tech companies and served as president and CEO. In 1998, he became a founding shareholder of an Internet company and took the company public within 2 years. His business and consulting experience includes management and technical consulting, smart city, cyber and network security, telecommunications and IT, managing technology companies, domestic and international business development, mergers and acquisitions, turnaround, investment capital, and strategic partnership in domestic and international environment. Dr. Singh has executed engineering, security, and IT businesses in 49 countries and has traveled to 81 countries. Dr. Singh's management consulting approach combines technical, organizational, and strategic management principles to create an effective and productive organization. In 2009, he joined with Dr. Pelton in writing *Future Cities: Designing and Building Smart Cities* as a project for the Intelligent Community Forum headquartered in New York City. Dr. Singh also teamed with Dr. Pelton to write *The Safe City: Living Free in a Dangerous World* and *Digital Defense: A Cybersecurity Primer,* which were published in 2013 and 2015, respectively. Dr. Singh has published five other books on telecommunications, IT systems, and security and was founding editor in chief of *Telematics and Informatics*, a global technology journal published by Elsevier. Prior to joining the business world, Dr. Singh served as a professor at Rutgers University. He also served as adjunct professor at the Kogod School of Business at American University and the School of Business at George Washington University. Dr. Singh resides in McLean, Virginia, USA, with his family.

Chapter 1
The Coming Age of the Smart City

"Our prime obligation to ourselves is to make the unknown known. We are on a journey to keep an appointment with whatever we are."

—Gene Roddenberry

The early 21st century is the time of disruptive technologies. Uber, a software company, is now the world's largest taxi service. Airbnb, another software company, is now the world's largest hotel company. Amazon.com and Ali Baba, both essentially dot.com companies, are the largest retailers. It thus should not come as a huge surprise that broadband, AI and IT systems are now poised to disrupt conventional ideas as to how to plan for, operate, invest in, and even re-invent the concept of what is called a 'smart city.' These powerful new digital technologies are strangely suited to being economically, socially and politically disruptive to every aspect of society—including urban life and city planning in contemporary times.

This book is a rough guide to what is meant by a smart city—both today and tomorrow. Its main mission is to make a plea that urban planners do not fall into the trap of thinking that the way forward is to throw technology at ever demanding problems that a city faces. No, we argue that the way forward to livable and effective smart cities involves 'smart planning' and judicious use of technology. This book is about the opportunities that a smart city can provide and the threats that it must overcome.

This is not a book about technology per se but having the wisdom and foresight in planning for better and more sustainable towns and cities. It is about the tremendous potential that can be unlocked and significant threats that can be overcome in this new digital age. This is a time that is filled with disruptive systems—economic, social, political and technological. Yet it is also replete with amazing new opportunities.

Most people—if they are honest—find things that are hard to understand and verging on 'nerdiness' quite boring. Just try to strike up a conversation at a cocktail party about differential equations, a new type of electronic ion propulsion system

© Springer International Publishing AG, part of Springer Nature 2019

J. N. Pelton, I. B. Singh, *Smart Cities of Today and Tomorrow*,
https://doi.org/10.1007/978-3-319-95822-4_1

for satellite stabilization, or the latest breakthrough in turbo-coding for efficient digital networking. Trust us, it doesn't work out well.

But the good news is that this particular smart city book charts a different path forward. We hope we have found the narrow and treacherous course that steers between being informative on one hand and dullsville on the other. If you wish to read about a viable way forward to achieve a better future for cities and how life might be lived in quite different ways in coming decades, we hope this is it. The trick is to explain these new trends and patterns of urban living without having to wade through reams of technobabble and intricate formulas. We try to sort through the threats that smart cities face from cybersecurity to technological overkill.

The *21st Century Smart Cities* seeks to be a good read. It is not a thrilling novel filled with sex, gore and intrigue, but it truly attempts to be engaging, informative, and entertaining. Fun facts range from what exactly are bitcoin and crypto-currencies and how block chain technology will change our lives. It explores the how and why of the Internet of Things (IoTs) and how it will soon evolve into the Internet of Everything (IoE). You will find out how living in a smart city will very likely transform your life by altering your sense of security, key educational systems, health care, your job, and your family life. Other than that, everything will remain pretty much the same.

Advances in smart city design and technologies will underscore how cybersecurity will become even more important to your life and your sense of security. This book takes you through ever key aspect of the evolving smart city and then ends by giving you our top twelve tips on how to live a more rewarding and secure life in this unfolding world of tomorrow.

Interesting, informative, exciting, and perhaps occasionally even amusing—these were the watchwords that we adopted as our mission statement for this book. If we are lucky we might even find a few ways to make it fun and exciting. We might be pushing it to say that it is fun, but perhaps sometimes there can be a chuckle or two.

What we are shooting for is a book that is filled with some new and intriguing facts about life, jobs, and existence in a future urban world. We pose a number of challenges for civic planners to consider and puzzle over. We even explore a few instances where smart city aspirations have gone awry and add in a dollop of political intrigue that comes with 'trolling' and cyberattacks on cities of the future and democratic societies. We thus make a sincere effort to explore some of the big challenges concerning the future of life on Planet Earth. By 2050 the world will be more than 80% urban, dramatically up from it being 53% urban today. This surge in urbanism and the rise of megacities represents perhaps the most important, and perhaps most dangerous, global trend in the world today.

We will explore the world of megacities, which are larger in population than many of the countries combined that exist in today's world. We will see how more and more megacities will become much larger than is optimum for efficient governance. There is a point where super density exceeds an increasing economy of scale and efficiency. Several times you will hear in this book that suburban sprawl is bad, urban density is good, but super density is bad again. It's bad for quality of life. It's bad for security and responsiveness to natural and human-generated disasters. It's bad for civic participation in building a better tomorrow.

This is only one of the oddities of this urban world of tomorrow. Our mission is to explore how these giant cities will adapt to the needs of their huge populations and their giant budgetary and service needs. Our top focus will thus be on these enormous cities and the need to create new, smart meta-cities that will surround these 21st century "city states." How can we help chart a future in which new meta city become more efficient, more secure, more livable, and more economically and environmentally viable? These are central to our discussions that follow.

It is vital to consider the experience drawn from emerging smart cities around the world. Many of these lessons learned are the essence of this book. Also key are the highly informative databases of best practices collected by entities such as the Intelligent Community Forum in New York City. This key organization has now collected key data from more than 300 smart cities from around the world. These and other narratives will enrich the fabric of our tale.

Let us start by saying what our idea of a smart city is. A smart city is not a thing, nor a technology, but a process that combines various elements together in a creative way. The seven elements key to creating a smart city are summarized in Fig. 1.1, describing the vital aspects of a smart city.

A smart meta-city system can be created within an existing and well-established city, or as one or more new towns at the edge of a large city. Alternatively, efforts can be undertaken to transform a megacity into a smart city, but this is the largest challenge of all. We believe that these satellite meta-cities, developed primarily on the edges of today's gigantic megacities of more than ten million people, will be vital to enhancing the livability and security of the megacities themselves as they too are transformed. Telework and 'smart' transportation systems will be key aspects of these transformations.

We will show how various communities around the world are today leveraging broadband communications systems, cybersecurity concepts and smart city planning to make 21st century urban living better. It might be to relieve the snarl of traffic

Fig. 1.1 Seven key elements in planning for and creating a smart city. (Source: Presentation by authors to Arlington County on March 14, 2018)

jams, to reduce crime, to ease the scourge of smog and greenhouse gases, or to offer better employment and security to its citizenry. This is a book about real problems in today's cities, but also about inventing new tools and better solutions for the cities of tomorrow.

In essence, this book about smart cities is thus really about what humans want to do with their lives when global society reaches the peak of many millennia of development. We explore some of the issues that arise when we reach a state of global human achievement that Peter Diamandis has called the "Age of Abundance," or which Ray Kurzweil called "the Singularity." Will the cities of tomorrow be "smart" or "dumb"? Will they be livable or quite overcrowded? Will they be functional, enjoyable, or perhaps both?

We also have to be honest. This book about smart cities does, on occasion, talk about technology and urban problems. We explore what life will be like when the world is over 80% urban and automation has redefined work and 90% of communications in the world will not be between people but between machines in the world of the Internet of Everything. Smart does not automatically mean better, more livable, or more secure. We have to work—and work hard—to make our cities places where we would want to live and raise our families. Technology is not a panacea. Technology provides improvement in the quality of life only with smart planning and clear thinking.

There are several things we can say for sure. This future urban world will be rife with significant change, as will be seen in the following:

- Social, economic, and cultural changes will occur rapidly.
- Human-machine interfaces will be critical to security and progress.
- Security will be a challenge—particularly cybersecurity.
- Lifelong education and retraining will become a way of life and health care an enormous challenge.
- Multiple job changes and careers will be commonplace as we cope with super-automation.
- Significant societal challenges will include longer life, challenges to individual privacy and perhaps democratic freedom.
- Technological and cyber challenges will likely require coping with "future compression," threats from cyber-criminals and even attacks launched by techno-terrorists and cyber-attacks on weapons of mass destruction.
- Concerns with increase with mega-problems such as climate change challenges, over-dependence on automated systems and artificial intelligence, changing global demographics, information overload, the digital divide and mass migration and immigration.

Key technological changes that we can depend on seeing in smart cities will likely include many of the elements depicted in Fig. 1.2.

We explore issues such as what will our lives be like in the future? There are fundamental questions such as how we adapt to a future where cities are no longer a place just to live but a living—almost breathing—environment. How do we best interact with an animated city that is not only "smart" but sometimes intrusive and

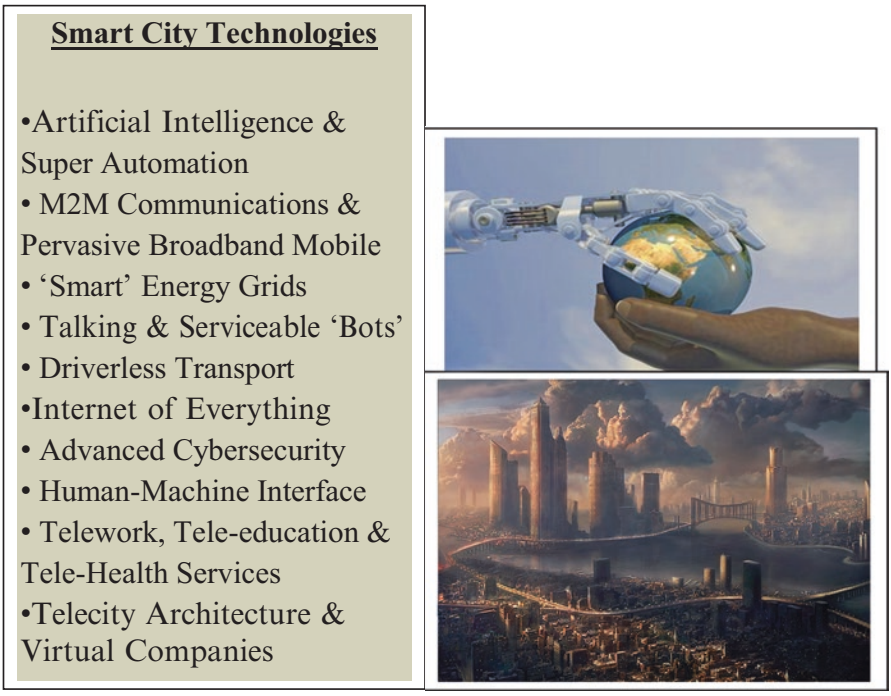

Fig. 1.2 Key smart city technologies. (Source: Presentation by authors to Arlington County on March 14, 2018)

even overprotective of its citizenry. If we are not careful, living in a smart city might curtail our privacy and potentially threaten democratic core values such as freedom, liberty and the pursuit of happiness.

This is because smart cities involve a little bit of everything, from social media and loss of privacy, to hackers and techno-terrorist attacks, from the latest developments in cloud computing and 'smart' homes and buildings and cars that can talk to you, to ways to save your life and lower your energy bills. In this new world, the divide between rural and urban populations, culture and politics that is already wide could become even wider with dangerous implications and results. So, hang on as we explore the opportunities and the challenges of the smart city.

Further Defining a Smart City

Many people have their own definition of a smart city and what it means to a populace. To our minds it is not defined by and through technology—although smart technology is still quite crucial. What makes a smart city is re-envisioning its design and functioning so that it can produce a better life and higher quality and

standard of living for its citizenry. This is to say that a smart city provides a community with improved health care and educational opportunity, higher security against natural and human-made disaster, social and political stability and freedom, economic prosperity and thriving businesses, and better housing, transportation, communications, networking, energy and all its other critical utilities.

The people in a true smart city have the opportunity for a safer, more well-rounded and prosperous life by being better equipped to enjoy the opportunity that a smart city provides to individuals, neighborhoods and the community at large. Figure 1.1 outlined the key elements of a smart city. These include: (i) fulfilling citizens' and business needs; (ii) creating environmental sustainability and a circular economy rather than a disposal economy; (iii) offering more jobs and competitiveness; (iv) getting citizen support for smart city planning; (v) improving infrastructure and resources; (vi) providing better technology and artificial intelligence; and (vii) providing better security. These seven concepts or goals are relatively clear, but executing them in an effective and systematic way remains hard. Indeed, coping with rapid technological change may be the most difficult challenge that society and cities will have to face during the span of the 21st century.

New Challenges Presented by Smart City Architecture

One of the key means of achieving a smart city will involve the use of the right technology in its planning and operation. This means that technology must be applied without disturbing key drivers of societal balance such as employment, out of kilter demographics and patterns of immigration, urban economics and basic aspects of safety and security.

Technology can provide tremendous new opportunity, but it can also entail vulnerability if that technology is abused or applied in a dangerous or distorted manner and without adequate backup emergency provisions. If you have ever worried about hackers and techno-terrorists in the past, just wait. In a future created by smart city infrastructure and broadband networks there will be an even greater threat of hackers and black hat cyber-terrorists lurking on the dark web than ever before. The history of counter-counter intelligence has proven this to be so for a very long time. Some claim that the new 'block chain' technology is the ultimate cybersecurity solution, but history suggests that this is not so.

The latest and smartest technology can also potentially bring a threat to jobs and lead to unemployment or underemployment. A recent study by McKinsey and Company of automation and employment in the United States has concluded that: "Over the next 13 years, the rising tide of automation will force as many as 70 million workers in the United States to find new ways to make money."[1]

[1] Danielle Paquette, "Study says automation could replace nearly a third of the U. S. workforce", *Washington Post,* December 1, 2017, p. A 13.

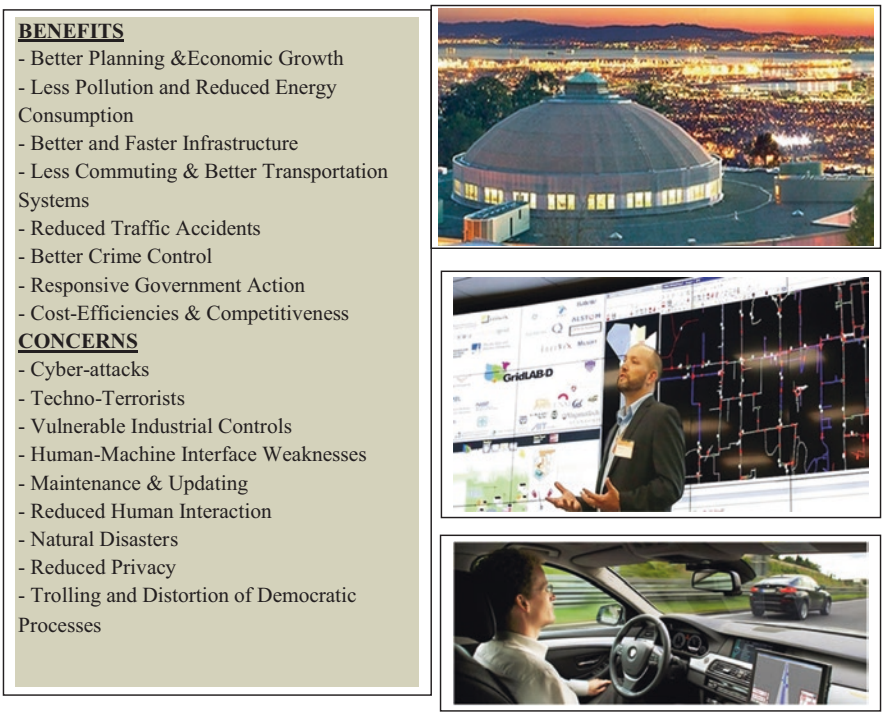

Fig. 1.3 Benefits and concerns associated with smart city technologies. (Source: Presentation by authors to Arlington County on March 14, 2018. All rights reserved)

This employment turmoil is due to what might be called super-automation,[1] a problem, of course, that extends not only to the United States but at least to all the developed countries such as members of the Organization of Economic Cooperation and Development (OECD). Vision and balanced goal-setting must seek an overall balance. Technology and automation are tools and not goals. The 21st century smart city must therefore involve thoughtful and balanced planning for the use and implementation of new technology, new infrastructure and better technology.

Figure 1.3 indicates some of the advantages and benefits of a smart city as well as some of the potential disadvantages to be guarded against.

This book explores the latest techniques and tools that make a modern smart city possible. It thus explores the latest in cybersecurity systems, new intelligent infrastructure and software. It also explores necessary administrative and political reform. We examine and even suggest some needed political, legal and regulatory systems to prevent the abuse of technology. In today's digital world it has become ever more difficult to employ smart system efficiencies while also defending freedom, privacy and liberties that are essential to preserving democracy.

Technical Challenges of Creating, Operating and Maintaining a Smart City

The technical challenges associated with a smart city today are enormous. It is ever more difficult to prevent cyber-attacks and find safe ways to employ the power of digital communications, cyber networks, information technology systems, artificial intelligence and advanced robotics. And these are just some of the key issues to be addressed in order to design, build and operate a smart city anywhere in the world. One can create a smart city anywhere. This is true whether it is in North America, Europe, the Middle East, Africa, South America, or Asia. Nevertheless, such a city must be conceived and adapted to its local culture and the needs of its citizenry, businesses, and national geography and its state of economic and educational development.

A true smart city must be planned on the basis of the right technology, the ability to adapt to changing demographics, education and health needs, employment, tax bases and adaptable infrastructure. New and sophisticated tools such as causal models, computer simulation runs and smart data analysis now makes such studies possible and likely outcomes predicted.

These key and integrated goals and objectives must consider dozens of vital factors, including safety, the degree of political, economic, and community cohesiveness, balanced employment, improved education and health services, vital and revitalized infrastructure and ultimately a social and urban design that can achieve all these objectives. These goals are not achieved through technology but by designing a smart city that is in harmony with its own inherent needs.

If the smart city is seen as a nail and technology is seen as the hammer, then the basic mindset is wrong. One must accordingly start with an organically developed and clear vision and then implement the goals and objectives. Technology must always follow those goals rather than create a paradigm that defines the future for technology's sake.

This harmony of basic smart city goals and objectives must mesh with the best digital technologies and smartware. Smart data must be employed that can help transform a city and apply the best technology in the best ways. The maxims, analytics and heuristic algorithms behind the effective use of smart data remain critical to any effort to create a better, safer and more intelligent city where people and neighborhoods thrive, technology is successfully deployed, and people are gainfully employed. When technology, effective planning and smart data are successfully analyzed and addressed, it can lead to a sense of true community. This means that social cohesion is nurtured, and smart practices and effective technologies can blossom across an entire city.[2]

There are many reasons why success is dependent on the wise and effective use of digital communications, artificial intelligence and information technologies.

[2] "Smart Data—What Is It and How Is It Different?" https://mail.aol.com/webmail-std/en-us/suite. (Last accessed Dec. 18, 2017.)

Cyber-attacks on digital networks and individual devices are becoming more sophisticated each year. As we transition in the decades ahead to a world primarily populated by smart cities with universal digital access we will be faced with the paradox of a life filled with more services and amenities but also an existence that is exposed to greater cyber risks. Expanded digital services, properly deployed, can lead to improved, more accessible urban opportunities. They can offer a vista of enormous new possibilities in education, health care, transportation, energy, security and good government, but only if such technology is deployed to achieve clearly defined goals, and potential negative effects are countered.

Indeed, new technological advances offer us a myriad of breakthrough opportunities. Yet despite these wonderful new prospects we will very likely be challenged by new forms of cyber-attacks, data protection issues and what is techno-terrorism. Other concerns must include a clear-cut case for effective security, employment, responsiveness to concerns and changing demographics, ethnicity and incomes of the citizenry, and responsiveness of educational, health care, first responder and all other governmental services to the needs of all neighborhoods. Finally, we must be attuned to how digital technology becomes at times almost overwhelmingly pervasive to the extent that it threatens personal privacy and democratic governmental processes.

One of the most intriguing paradoxes posed by the smart city is the use of smart data and artificially intelligent systems in the design and operation of the next generation of smart cities. These technologies can help with the creation of smart infrastructure that allows us to build more efficient, less costly, cleaner and safer ways to operate a city. But one must be careful as to what one wishes for. Especially consider the longer-term consequences and constantly survey the populace to make sure that they feel progress is being made and that personal privacy is not overly invaded.

Artificially intelligent and highly automated streets, highways, bypasses, rail systems, energy networks and systems, water and sewer systems and more can lead to unexpected consequences. These consequences can be realized in terms of lower employment, higher risks of cyber-attacks, privacy concerns and totally unexpected new types of social, economic, taxation, business, and political concerns. A smart city always has its finger on the pulse of the community. This can lead to new efficiencies but also concerns related to democratic processes, privacy, employment and jobs and human fulfillment.

Concerns About Full and Meaningful Employment in the Smart City

Kai-Fu Lee, Chairman and CEO of Sinovation, a venture capital firm that specializes in artificial intelligence, has noted that the newest technology that is moving us toward driverless cars, completely automated manufacturing and more will spread to every sector of the economy. In time, this will include health care, education, engineering and the operation and functioning of cities. He has said: “Unlike the

Industrial Revolution it is not taking certain jobs….and replacing them with other jobs…Instead it is poised to bring about a wide-scale decimation of jobs…."[3]

As noted in the book *MegaCrunch: Ten Survival Strategies for the 21st Century,* most service jobs are currently being converted by smart software into tasks that can be performed by machines. This book strongly advises: "The time to start adapting to a new ecosystem where machine labor replaces much of today's employment around the world is now."[4]

This admonition applies not only to business and national governments but to urban governments as well. The big problem is no one has a feasible economic or employment plan that all agree with. Microsoft entrepreneur Bill Gates has suggested that there may need to be a sort of tax on those who create the tools of automation in order to pay a form of cost of living compensation to those who lose their jobs to advanced robots and software algorithms that can outthink most service workers—including municipal employees. The issue posed by smart cities is thus much larger than just cybersecurity to protect smart infrastructure and utilities against cyber-assault. There is also the question of what do humans do when smart machines perform most of the jobs?

In short, smart cities and expanded use of IT systems and artificial intelligence can bring a longer and safer life, new economic opportunity, even amazing new opportunities such as travel to other planets. But the technology that provides us new prospects can, ironically, also create new risks and pose new economic and political challenges. Current trends suggest that we will continue to move forward at an ever-faster pace to create smarter cities that can open up these new vistas. In this transition we will not only fully embrace the Internet of Things (IoT) but then move on to the Internet of Everything (IoE). In this new world, cyber defense will, at once, not only become more difficult but also more essential. The need to cope with cyber threats will increase at an exponential rate. Only automated and smart cyber defense will allow us to cope.

Living in the World of Tomorrow

This transition to the world of tomorrow will be everywhere. Not only in terms of driverless cars, smart vaccines and DNA therapy against disease but also in terms of automatic controls for virtually every aspect of the infrastructure of the smart city of tomorrow. This means machines and artificial intelligence will help make operations of virtually everything "smarter," i.e., transportation systems, the electrical grid, water and sewage systems and natural gas distribution. This will also be the case for buildings and houses. Everything within the next two decades will likely be 'smart'

[3] Kai-fu Lee, "The Real Threat of Artificial Intelligence" *New York Times,* Sunday Opinion Section, June 25, 2017 pp. 3–4.

[4] Joseph N. Pelton and Peter Marshall, *MegaCrunch: Ten Survival Strategies for 21st Century Challenges,* (2010) PM Associates, London, U.K.

within modern buildings and homes, including all utilities, appliances and security systems. The trick is finding a way to make all of these intelligent systems reliable, safe, and risk-free against the assaults of cyber-criminals and techno-terrorists. The other trick is the redefinition of work and employment within these cities of tomorrow. We hope someday soon to find these answers, but to date no one has absolute answers to these problems. We would be lying if we said we had these 'magic' answers.

Recently experts in artificial systems, scientists and business entrepreneurs, notably Stephen Hawking and Elon Musk, have sounded the alarm against overly embracing artificial intelligence and intelligent infrastructure, especially in weapon systems. Some have even warned us against a future world that includes smart weapons systems that might be subject to hacker attacks. The use of smart weapons and intelligent defense-related devices are beyond the scope of this book. Nevertheless, this is yet another policy area that politicians and urban planners should be clearly aware of as well.

In short, although this topic is not probed in this book, AI in defense systems is another area of concern and interest that is important to the future. As we develop increasingly smarter IT systems, these types of concerns will be an area of increasing concern and interest.[5]

Therefore, we see an ever-growing need exists for more effective cybersecurity and defense systems against the abuse of IT systems in the smart cities of the future that are now possible to design, engineer and implement around the world. Some believe that this digital threat is increasing because cyber criminals are getting craftier, better schooled in hacking and have easier access to the latest tools because of the "dark web." And indeed, this is a significant and very real part of the problem. These cyber security threats will grow as usage of the dark web expands and access to malware becomes easier. This we know from decades of experience, that cyber criminals will continue to devise new ways to misuse IT and AI systems.

But the true key to the rapid growth in cybercrime is that the global digital ecosystem is itself fundamentally changing. This change is significantly being driven by the rise of smart cities and the expanded use of digital systems around the world. Some believe that the spread of smart cities is restricted to only a few of the world's most economically and technologically advanced countries. This is not the case. The governments of India and China, as well as dozens of other newly industrializing countries, are now spending many billions of dollars to create a myriad of smart cities. These are both new as well as totally retrofitted existing cities that are being transformed with an amazing array of services from tele-education, tele-health and on-line governmental services, to smart utilities, tele-security capabilities, "smart" power systems and intelligent transportation systems.

[5] Peter Holley, "Artificial Intelligence Can Unleash 'Revolution' in Warfare Tech Leaders Warn" *Washington Post*, August 22, p. A14.

A New Digital Ecosystem

We are moving from a world where humans are not necessarily in charge. The digital world is more and more automated. This is the case because humans are too slow and are not able to handle the complexity that is associated with the smart city, where every second millions of decisions must be made, and soon that number will increase to billions.

In the new digital ecosystem, machines will be in charge of many aspects of our lives. Transportation routing, electrical power flows, lighting, water and sewage flows, operation of elevators and escalators, operation of traffic lights, and thousands of other transactions will be controlled by industrial control systems and artificial intelligent algorithms. These systems will be safer, more reliable and much more efficient.

The prime role of cybersecurity in this new world, where the Internet of Things morphs into the Internet of Everything, is to make sure that cyber-criminals and techno-terrorists do not take control of our digital machinery to do us harm or disrupt vital services. If we can keep the cyber-criminals in check, the smart cities can provide us with schools that are more efficient and reliable and better health care. We can have energy and transport systems that are environmentally more sound, effective, economical, and safe. One of the keys will be to provide safe-guards. This is so that machines and AI systems are prevented—by such means as human machine interfaces (HMIs)—from doing damage to the safe and effective operation of the smart cities of tomorrow.

We are thus more and more living under a new digital ecosystem that is being shaped by the cloud, the architecture of digital networks, the Internet of Things, and increas-ingly smart automated industrial controls and supervisory control and data acquisition (SCADA) networks. With these machines and computer-based algorithms in charge of operations they can be more than a hundred times more environmentally sound and efficient. The hitch is that key aspects of digital defense must be significantly rethought.

This book is about the new digital ecosystem that will represent the "brains" of smart cities. We will explore new methods and procedures for coping with new types of digital risks. We will help to explain new strategies for undertaking cyber-defense in this new largely automated world. It is not possible to mount effective cyber defenses without understanding this fundamental shift in what we call the new digital ecosystem. This new approach to digital defense must become part and parcel of the smart city of tomorrow.

When Is a Community a Smart City

The Intelligent Community Forum, with its headquarters in New York City, has recruited a global network of judges that each year designates 21 cities as intelligent cities. These are then narrowed to the top seven and ultimately one overall top winner is chosen.[6]

[6] The Intelligent Community Forum March 2018, www.intelligentcommunity.org.

Some of the criteria that the Intelligent Community Forum uses in this selection process include the following.

Sufficient Broadband Networking Services

The judges consider whether there are readily available broadband networks sufficient to support governmental, medical, health care and school systems as well as private households and commercial enterprises. This evaluation process considers at what cost services are provided and under what operational conditions—including whether there are, for instance, competitive systems.

Smart Public Transit and Automotive, Rail and Air Transportation Systems

This evaluates the quality and extensiveness of coverage of public transit systems as well as the nature and intelligence of automotive, rail, air and bicycle transit systems in terms of their controls, responsiveness to changing patterns of use throughout the day and week as well as their security.

Smart and Versatile Power Systems and Degree of Sustainability

The viability of networked services depends heavily on reliability of electrical power systems and the back-up capabilities for emergency services such as 911 call centers. A key concern is whether the electrical power system is secure against hacker attacks.

Effectively Managed and High-Quality Utility Services (i.e., Water, Sewage, Gas, etc.)

The modern smart city must not only have all types of key infrastructure related to utilities (i.e. water, sewerage, gas, and electricity) operating at maximum efficiency, using effective and protected industrial controls (i.e. SCADA or Supervisory Control and Data Acquistion), but these must operate under effective security measures and back up control systems.

High-Quality Educational Systems

The viability of a community—especially in terms of its political, economic and cultural future—depends on a quality educational and training system geared to the needs of its population.

Improved Health Care Systems

A community is heavily dependent on a quality medical care, health care, sports and athletic programs that allow its citizenry to remain healthy.

Community Spirit and Political Processes to Increase Citizen Input in Decision-Making

The development of new and capable IT infrastructure and software that ensures its effective operation is key, but a political process that allows the definition of systems that allow a city to operate effectively and meet civic objectives is at the heart of a true smart city. A city without effective citizen input and strong support for creating a better future for its entire citizenry will likely not succeed in the longer term.

Housing, Jobs and Employment

Other key aspects of a successful city are those capabilities and efforts aimed at improving and increasing available housing, jobs and meaningful employment, and fiscal stability as well as achieving sustained financial and economic growth. These represent key indices to monitor in order to assess the how smart technologies are helping to create a better city and a better future.

Fiscal Stability, Quality of Financial Planning and Economic Expansion

Closely linked to jobs and employment factors are financial well-being and sustainable growth based on a vibrant economy and a viable tax base. This requires an optimum balance within a community. A desirable urban condition is where there is some growth and expansion but not at excessive rates. Population growth at greater than one to two percent per annum can be increasingly problematic. Many of the world's

largest cities, particularly megacities of ten million or more inhabitants, have exceeded the size associated with sustainable growth and the ability of urban infrastructure to expand to meet overheated demand. The transition from overcrowded megacities to broadband-linked meta-cities is one way to make the cities of the future smarter.

Effective and Secure Automated Control Systems for All Infrastructure

Automated industrial control systems (such as so-called SCADA networks), computer software algorithms, robotics, and artificial intelligence can improve efficiency, reduce the cost of government, and allow the smart city to blossom. These automated systems can help to optimize energy efficiencies, relieve rush-hour conditions, improve transportation systems, deliver more effective utility services, and much more. But such systems must be secure against cyber-attack and geared to the needs of the citizenry, or these automated systems will ultimately fail in their mission. In the smart city security is increasingly important and essential to ultimate success.

Artistic, Cultural and Library Services

Some urban leaders look to their success and find it in controlling finance, budgets and taxes, but in a true smart city the objectives need to be broader. Success in all of the above criteria need to be supplemented by attention to needs related to the arts, culture, sports and athletics, libraries, and citizen involvement in their community. These factors can be equally key to a smart city. Controlling infrastructure, taxes and financial expenditures is just one aspect of success within a smart city.

Sustainability of Growth and Development

Balance is everything. A smart city will ultimately succeed in the longer term if it has a sustainable arc to the future that allows it to succeed in all its key dimensions. These include economics, employment, population growth, housing, health and education, political governance, citizen involvement and cohesion, efficient infrastructure for utilities, transportation, communications and IT systems, and more. These need to expand to meet citizen needs and still provide a healthy and sustainable environment while also remaining secure and peaceful. Most of all, this means creating a circular economy. Such an economy minimizes the waste of resources and pollution and abandons the principles of a linear economy. Such a linear economy is based on continuous throughput and the so-called ‘take, make and dispose’ model of production.

Effective and Inclusive Long-Range Planning to Accommodate Growth

Key to most urban centers and their ultimate success are the following seven drivers: (i) population; (ii) environment; (iii) energy; (iv) government (v) economy; (vi) cultural/religious and linguistic coherence; and (vii) technology. An effective smart city will always be conducting longer-term planning to create a better future for its citizenry. One cannot achieve effective planning by focusing on a single factor such as technology or economic growth or controlling taxes. A success plan will consider all of the needs and express these in the form of critical factors. As is the case in most business and civic ventures success typically comes from seeking balanced and sustainable growth to meet the needs of all concerned.

Long Range Vision

Urban vision and key strategic goals are the last elements that are essential to the continual improvement and positive evolution of a community. If the city leaders, the public employees and the community have no purposeful view of the future and where they would like to community go, then they will never get there. A set of truly long-range goals that is shared within a city is a crucial aspect of a true smart city.

These are the many types of criteria that the Intelligent Community Forum uses to judge which are the best smart cities around the world. The process draws on the wisdom of a broad-based number of international judges. These criteria represent one way to begin to define what a smart city is. Of course, there are other ways that might be used to define and create an intelligent community.

Drawing on Best Practices from Around the World

The Intelligent City Forum also maintains a database that documents the best practices as gleaned from the actual experiences of over 400 cities around the world. Drawing upon these best practices and implementing them within an urban planning process might be considered another way to undertake to create a smarter city. These smart practices draw on the urban design and operational systems applied to smarter transportation, education, health care, management of city utility systems and improved environmental sustainability, better government system operations with regard to taxation, zoning, planning and services of all types. The following of these practices can make city operations more efficient and timely, more responsive to citizen and business needs, help expand jobs and improve the city tax base, and generally improve the provision of vital services to the citizenry and its business community.

In short, smart cities strive to be better in virtually every dimension, whether this means higher employment, better roads and public transportation and communications, a better educated citizenry, improved health care, a cleaner and more sustainable environment, improved utilities and infrastructure, and better government and responsive public services. Much of this is achieved through improved IT and broadband telecommunications systems, responsive computer systems and improved software, artificial intelligence and expert systems, robotics, and smart technologies. Yet, the bottom line is that without good government and responsive political and economic systems one does not achieve a smart city able to sustain public support.

Many of these ideas about how to create a smart city and sustain and improve it over time are captured in the following two books: Joseph N. Pelton and Indu Singh (editors), *Future Cities* (2009), Intelligent Community Forum, New York, and Indu Singh and Joseph N. Pelton, *The Safe City: Living Free in a Dangerous World* (2013), Emerald Planet, Washington, D. C.[7]

Applying Digital Technology Wisely

Every country with its unique social, economic, cultural, linguistic, and governance structure will have a similar approach to creating and sustaining a successful smart city. However, there can be many differences of approach. The design of a successful smart city can vary significantly from country to country or even within different regions of the same country.

For example, the two leading examples of a smart city—Singapore and Dubai—are very different from each other. The fundamental differences are not related to technology but to strategic and economic objectives. Both city-states are modern, progressive and thriving places for even casual visitors. Both achieved their objectives without sacrificing their social and cultural history. A smart city can be funky, off-beat, glitzy, or even subdued, but it must be perfecting itself against its own vision of greatness.

Nevertheless, the fourteen criteria spelled out earlier in the previous section are useful to consider and adapt to a particular country and culture. The emphasis given to the criteria might vary, but all of these criteria are worthy of sincere consideration.

The important thing to consider is that appropriate and precisely crafted use of digital technology and software is central to creating the smart cities of the future. Yet the successful application and use of digital technology and intelligence also remains a two-edged sword. Digital technology, improved IT systems, robotics and artificial technology and industrial control systems can all help to improve every aspect of future smart cities, but without effective cyber defense systems, these tools can also serve to expose these high-tech urban centers to risks and a wide range of cyber-attacks. Each

[7] Joseph N. Pelton and Indu Singh (editors), *Future Cities* (2009) Intelligent Community Forum, New York and Indu Singh and Joseph N. Pelton, *The Safe City: Living Free in a Dangerous World* (2013) Emerald Planet, Washington, D.C.

improvement in the technology can also expose a potential area of risk. Once technology is invented and proven to be useful, it is difficult to un-invent it.

High-speed jets, trucks and automobiles speed up transportation but create pollution problems. High-rise buildings with elevators provide more efficient homes and offices but expose us to the risk of fire and natural and manmade disasters. Virtually all technologies give birth to new opportunities and efficiencies, but also expose some new element of risk. IT networks, artificial intelligence, robots, and industrial control networks are no exception.

Our book examines the ways that the latest in IT and AI technology is opening the door to new opportunity, but also might be leading to new risks that cyber-defense mechanisms and practices are needed to avert problems that will arise in the world of smart cities and the technologies they need to operate.

The Rate of Accelerated Change

The primary step forward requires new thinking. One must start with an improved understanding of the complexity of modern cyberspace environments, and the ever-expanding interconnectivity of the various types of worldwide systems operating within cyberspace. Studies conducted by Intel and its subsidiary Wind River have produced credible estimates for the period that extends from the end of 2016 to the end of 2020 that there will be a 50-fold increase in the amount of stored data. This same study has also estimated that the amount of data generated from machine-based systems such as the Internet of Things will increase by a factor of 15 times in just a 4-year period. After that things will likely accelerate even faster.[8]

If these estimates are even close to being right, we will see the need to upgrade and increase processing platforms, along with filtering and pre-processing software, to slow down input from the "edge" into centralized processing capabilities. Perhaps most significantly we will have to use cryptography and new types of security systems to make these digital networks, driven by Internet of Things machine-to-machine exchanges, less vulnerable to cyber-attack.

We must rethink everything we know about digital operations, as these machine-based systems take over our world. As automation steps on the gas and powers our world into new speeds of operation we need to know how to apply the brakes. Otherwise we lose control. Cyber-criminals and cyber-terrorists can hijack our world and play chicken with our security. Ironically greater efficiency can also mean greater danger.

[8] The Internet of Things for Defense, A White Paper, Wind River—An Intel Company, October 2015. http://www.windriver.com/whitepapers/iot-for-defense/wind-river_%20IoT-in-Defense_white-paper.pdf.

The New Scale of the Global Digital Ecosystem

In brief, we are currently not equipped to cope with the degree of change that is coming. Of the projected devices that will generate the massive increase in data that is stored in computer clouds or flows on data networks, perhaps as many as 85% are not currently connected to the Internet or various Intranets now operating. This massive sea-level change is changing the entire ecosystem within which cybersecurity and cyber systems must operate.[9]

In the 1970s all known information stored in all the world's databases could be reckoned in terms of petabytes of information. A petabyte is 1000 trillion bytes of information or, if we write it out, an impressively large 1,000,000,000,000,000 bytes. If we think of the worldwide databases essentially stored in hardcopy paper files and various types of tapes and video and audio as an elephant, computer-based storage of information was a gnat on the tail of the elephant. Vital security and military information was physically protected within secure facilities, and any theft of secure information was extremely difficult and usually easily detected.

Today, if we think of information and data stored in traditional modes such as paper, microfilm, transparencies, slides, video and audio tapes as still being an elephant, then computer-based data would be a creature as large as the Rocky Mountains, and in the next few years that would be growing to the size of the Moon. Coping with the Global Digital Ecosystem today can be reckoned in terms of new and unfamiliar terms of exabytes, which are a million terabytes. It was recently estimated that all the words ever spoken by humans represents a total of 5 exabytes. But now we are developing machine storage systems that are even larger than zettabytes. A zettabyte represents a billion terabytes. In 2012 it was projected that by 2016 Internet traffic would reach 1.6 zettabytes—a level it greatly exceeded. It must be noted that most of that traffic was to support visual information in the form of TV shows, movies and quite a bit of porn. Sadly, porn may be the biggest use of bits on the Internet.

This explosive use of the Internet means that we are on the cusp of coping with globally stored information that can be reckoned in terms of not terabytes, petabytes, or exabytes, or even zettabytes, but yottabytes, which means a trillion times a trillion bytes of data. The facility that the National Security Agency has recently built in Utah is reportedly able to cope with the storage and processing information on the incredible scale of yottabytes. This is the size of what we characterize as the Global Digital Ecosystem of 2020, and it can be safely said that coping at this level of information for humans is both difficult and more than a little scary.[10]

[9] Ibid.

[10] How Big Is A Petabyte, Exabyte, Zettabyte, Or A Yottabyte? High Scalability http://highscalability.com/blog/2012/9/11/how-big-is-a-petabyte-exabyte-zettabyte-or-a-yottabyte.html.

Cybersecurity in the New Age of the Global Digital Ecosystem

The first step is thus to achieve a better understanding of digital networks and their strategic and economic importance as well as their exponential growth at unprecedented levels. The next step is to develop new methods and principles for the following three objectives:

- Creating better ways to defend these systems from cyber-attacks, including design of smart cities to include improved cyber resilience.
- Developing a systematic way for reporting and understanding intrusions in terms of where they come from and how to better protect against these attacks.
- Implementing improved methods for swift recovery from these assaults on private, corporate, governmental and defense-related networks, with a minimal loss of vital digital data and the ability to target those mounting such cyber-attacks.

This book provides an in-depth understanding of the theory and practice behind smart city development and also explores the key cybersecurity issues needed to defend it.

The core of this book covers the following:

- A review of the planning and implementation processes needed to create a safe and smart city and an analytical discussion of the building blocks needed to achieve future success.
- The need for the right tool sets. You truly need good causal modelling and heuristic algorithms and smart data analysis. Without such tools it is hard to detect urban problems, make the right investments and address key issues in a timely way.
- A way to detect and exploit new opportunities by using the best technology, creating the right smart infrastructure and software that can make a city better.
- An improved approach to cyber-defense. This can perhaps be the most difficult of all. Cybersecurity is particularly hard in an increasingly interconnected world and the expanded vulnerabilities that come with the Internet of Things, industrial controls, and automated and SCADA command systems that now exist throughout the whole of modern society. It is constant hand-to-hand, anti-virus to anti-virus and firewall-to-firewall combat. Unfortunately, there is expanded use of ever more disruptive digital tools.

The Importance of an Interdisciplinary Approach

In this book we not only focus on the interconnectivity of modern systems but also use a holistic and interdisciplinary approach to what might be characterized as digital ecosystems. The attempt is to present a better understanding of the overall context of cyber defense that can be best realized by taking an interdisciplinary approach. Thus, readers will benefit from the results of ongoing research and the

development of new protective strategies for digital networking. This applies to all forms of transmission media and the various types of devices and systems that are now vulnerable to criminal or terrorist assault.

Understanding the Language

Finally, it is important to note that one of the many, many challenges in addressing the new digital ecosystem and the lexicon of the smart city is the complexity of the terminology, acronyms and other phrases used around the world in addressing this increasingly complex subject. The extensive glossary provided at the end of this book tries to span this wide range of phraseology and acronyms now in use in the fields of urban planning, smart city design and technology, computer science, networking, cybersecurity, telecommunications, and regulatory control mechanisms and agencies. Even this rather comprehensive glossary is not complete, and here one might seek assistance from Internet searches. Caution is urged in the use of acronyms because sometimes an abbreviation may have more than one meaning and terms current even last year may be now out of date.

Here, now, is a preview of chapters and how the book is structured.

Chapter 1: The Coming Age of the Smart City

This chapter has introduced some of the generic concepts defining the smart city and identifies some criteria on which a smart city might be judged. It defines some key terms, concepts, technologies, tools, infrastructure, and software that are central to chapters that follow. It also notes some of the special challenges related to cyber defense and why it will be increasingly difficult as we make the transition to the age of universal networking and move from the Internet of Things to the Internet of Everything.

Chapter 2: The Challenges of Envisioning and Planning a True Smart City

The latest fad is for major cities, city managers, or city planners to slap the label smart city on their community, upgrade some computer installations, IT networks or broadband telecommunications systems and declare success. The truth is that the pathway to creating a true smart city is long and difficult. Plus, it is a goal that will never be completely reached because one of the essentials of a smart city is to plan constantly to improve a community at all levels. This is not a single improvement to be marked

off in a "once and done" manner. It is to create longer term plans across all of the areas noted in this chapter and to make steady improvement. The Arlington County community, which has been officially noted several times as an "intelligent community" by the Intelligent Community Forum (ICF), has for instance a 40-year Community Energy Plan that it is constantly seeking to improve. Effective specific goal-oriented planning at the short, medium, and longer term is the earmark of a smart city.

Chapter 3: The Critical Infrastructure and Software Needed to Build a Smart City

It is essential to convert a vision and detailed planning and budget allocations into the urban infrastructure that is integral to a well-functioning smart city. The various infrastructure elements of a city need to be conceived and viewed as an interactive system. This must include a well-designed health and educational system, a carefully crafted transportation system for a city, a broadband network for telecommunications and networking, plus a modern energy-generation and distribution network as well an environmental control system and the other key utilities, such as for water, sewage, trash removal, etc. This chapter addresses how a modernized infrastructure that is planned, engineered and implemented on an integrated and interdisciplinary basis can function better, be more efficient and avoid needless redundancy and waste while also being more resilient.

Chapter 4: The New Age of the Smart City: Why Cyber Defense Is of Key Importance

Chapter 4 provides key definitions of cyber defense, cybersecurity and cyberspace within the context of the smart city. It highlights the importance of understanding a growing degree of network interactions and complexity that we call the new digital ecosystem that will be at the heart of the smart city. The main characteristic of this new digital world is that its operation will be driven by automated systems, digitally based algorithms and artificial intelligence rather than by human control. This chapter thus seeks to explain the new era of interconnectivity between the digital and human-controlled worlds. This changed digital ecosystem will allow unparalleled growth in digital interactions that will unfortunately increase digital vulnerabilities around the world and especially smart cities. In the age of RFID and the Internet of Things, trillions of smart devices will interact over an unimaginably large number of electronic and photon-based links. As a consequence, cyber density will become exponentially larger throughout modern society. Thus, cybersecurity will become more difficult to develop and implement on a timely basis.

This chapter examines the cyber-security challenges in the following terms: interconnectivity, complexity and the growing diversity of advanced technologies. The largest challenges will be to address the volume of digital interactions as well as the increased level of use of artificial intelligence in digital networks. An effective cyber defense also requires a multidisciplinary research approach, with not only in-depth knowledge in terms of IT, software and systems engineering but also consideration of relevant economics, law and social sciences. This chapter thereby describes cyber defense from a system perspective, i.e., taking a holistic approach to a "living" ecosystem that will be at the heart of most smart cities.

Chapter 5: Using Smart Data for City Planning and Design

Two of the hot buzz words of our times are data mining and big data. This process examines large databases and, through analytics, unlocks hidden meanings and reveals key trends. The latest thinking on this subject is to develop causal models and heuristic algorithms involving major change agents to examine how data involving key variables drives change within a particular system. One can use the "smart data" to see how various types and rates of change affect an urban community. One can, for instance, put together a causal model of a community based on key drivers such as education and health care system requirements, energy, environment, transportation, communications, zoning, housing and buildings, economic throughput, jobs and employment, industrial base, etc., and then see how those various drivers of urban change react when one varies rates of population growth, aging of the citizenry and workforce, etc., against these various institutional components. As a community grows, ages, and diversifies its economy, it must have infrastructure that can change to meet altered requirements. This type of smart data analysis is key to the evolving capabilities provided within a smart city.

Chapter 6: Protecting Privacy and Democracy in the Smart City

This chapter investigates the consequences and potential downsides of more automation, more sensors and more implementation of artificially intelligent and "aware" information processors that can potentially adversely affect social, economic and political conditions. It has been reported that some countries and some commercial organizations such as Ali Baba, a Chinese-based online buying service, are collecting huge databases to "rate" citizens and their behavior patterns. Others are installing millions of cameras and sensors to be able to track or locate people using a combination of sensors and computers with facial recognition software. The key question is this: Is it possible to increasingly automate key software and use AI-based

logic systems to operate and control infrastructure without also limiting or perhaps greatly impinging on a citizen's rights to personal privacy, freedom, liberty and democratic principles and processes?

Chapter 7: A 21st Century Smart City and Mobility

Chapter 7 charts the rapid expansion of broadband mobile communications and mobile applications, including instant credit card payments, broadband entertainment delivery, and a variety of texting and e-mail services, which represent a key area of significant cybersecurity concern. The opportunities are enormous for cyber criminals to intercept messages, abuse financial transactions either to steal money or assets or acquire information that allows for the extraction of money. This chapter will address the trends in this area and the security measures that can be applied. Consumers should use unsecured public networks as seldom as possible and with great caution. Further, Apple Pay and similar instant payments can be hacked in a variety of ways. There is often a price to pay for instant gratification, whether it involves paying for an illicit or licit service.

Chapter 8: Smart and Safe Control Systems for the Smart City

Chapter 8 considers the ever more critical functioning of the day-to-day governance and increasingly autonomous control of urban infrastructure and vital operational systems. The reach of remote control systems is now almost everything. Their impact—and potential vulnerability—is now sweeping and thus of great concern. It extends from vital pipelines to traffic signals, from warehouse inventory systems to electric power grids, from water and sewerage systems to "smart" roadways and electronic banking. This automation of a vast range of key services allows significant increases in productivity and enormous labor-saving capabilities. In virtually all cases it increases safety and continuity of operations and resilience. But this automation of vital services also creates new opportunities for accidental commands and deliberate actions by disgruntled employees, cyber-criminals and cyber-terrorists to throw a wrench into normal urban operations. It is discouraging to find in systematic audits of SCADA systems that control many cities' operations and vital infrastructure that the security codes in use are the ones provided by the computer network equipment supplier. Command and control of smart city operations are of key importance. Such capability can improve effectiveness, efficiency, reliability, resilience and safety of operations.

Chapter 9: The Smart City Floating Safely on the Cloud

Chapter 9 explores the importance of cloud computing and how its reach is increasing, in part due to the very rapid increase in machine-to-machine communications and acquisition of data from the Internet of Things that will morph into the Internet of Everything. It also allows flexible, cost-effective platforms for services over the Internet or via closed enterprise intranets. This chapter provides definitions and explanations of the benefits and security risks associated with using the cloud for various types of digital operations. Particular risks are then described with regard to third party outsourcings well as issues with regard to the maintenance of cybersecurity and privacy. This chapter emphasizes the importance of data analytics.

Chapter 10: The Challenges and Opportunities in the Evolution of the Internet of Everything

Chapter 10 gives special focus to the unique security requirements related to the Internet of Things (IoT). This chapter starts with some key definitions and fundamental principles of coping with the globalization of IoT. These security concerns are presented in the context of defense and governmental networks as well as protective measures for corporate and publicly accessible networks. This chapter describes how mobile devices, satellites and terrestrial networking systems are used in complex digital systems including enterprise networks, industrial control systems (ICS) and totally new applications such as control of autonomous vehicles. The IoT creates unique new opportunities for an end-to-end ecosystem that also gives rise to security and resiliency issues. Risks become larger when the decisions can be made both automatically and in a distributed manner.

Chapter 11: Coping with the Dark Web, Cyber Criminals and Techno-Terrorists in a Smart City

Chapter 11 describes network security challenges and how they are expanding in now globally accessible cyberspace. This chapter analyzes the impact of cyber-attacks carried out within complex systems such as SCADA, the Internet of Things, and mission-critical military systems. It also discusses how to assess, measure and calibrate the cost of cyber-crime, cyber-attacks, cyber-defense and cyber-network security. The range of malware, stolen credit card numbers, and other tools of cyber-crime that can be purchased through the dark web keeps growing. Law enforcement is always, it seems, one step behind. Steps like the Eurocard, Mastercard and Visa (EMV) smart chip cards are a step forward, but protective systems are, in general, too little, too late.

Chapter 12: How Nations and Smart Cities Can Cope with Cyber Warfare

The protection of the smart city against disgruntled employees, natural disaster and cyber criminals out to make a buck by using malware to extort money via such an attack virus like "WannaCry" is one thing. Attacks that amount to cyber warfare by hostile nations or terrorist groups are another. This chapter addresses new types of threats that can cripple a city and its vital infrastructure. There are new vulnerabilities that can come with technology such as the Internet of Things, but also new opportunities for urban defense by such means as blockchain encryption that Singapore, Dubai and other cities are using to defend their vital records and speed up the efficiency of urban operations.

Chapter 13: Flexibility, Vision and Foresight in the Planning of Smart Cities

The smart city must be designed for flexibility and a good deal of future vision. This flexibility must be a key component in the planning of vital infrastructure that will likely be controlled and commanded by cyber networks in the future. Thus, planning and command systems must be designed to allow redeployment of resources. Significant changes in transportation, education, healthcare, and various utilities must be anticipated as well as changes in the make-up of urban populations. Many of the factors that supported the desirability of large populations, such as readily available labor for farms and workers in factories, no longer apply. Changes in transportation such as shared ridership, self-driving cars and companies such as Uber and Lyft could help reshape cities of the future.

The form of vital infrastructure for transportation (i.e., air, rail, public transit, automotive road and traffic systems and even elevator systems) could all change. Further, many forms of current utilities (i.e., water, sewage, gas, HVAC, and electrical power plants, including nuclear power plants) may, in future years, be called upon to respond to changing needs of the populace. Thus flexibility, modularity and ability to respond to natural disasters and even terrorist attacks must all be considered to be a part of the planning processes for smart cities of the future.

In planning for these cities of the future, a key process must involve the consideration of a wide range of what if questions? What happens if employment patterns were to change? What if driverless cars change our road and highway system needs? What happens if the networks we plan today must serve a populace with much different needs and characteristics? Can we design more flexibility or safety into our infrastructure and urban design? Can smart planning better help to shield our cities from some sort of natural disaster or attack—either of a cyber or a physical nature? Such flexibility in urban systems design could prevent loss of life or a major accident

or allow much more effective emergency response. Unfortunately, planning officials or zoning decisions often fail to consider the implications of an earthquake or a fire when they approve the building of skyscrapers over 100 stories in height. In the age of broadband telecommunications, massive urban density has many downsides that include a great loss of flexibility and responsiveness.

Chapter 14: The Smart City—Build It and They Will Come

This final chapter recounts and emphasizes the most important elements of the book and provides a summary of these elements. It indicates twelve key conclusions that are the top areas where future research and better city planning must be focused. Ultimately, in addition to new IT technology, automated infrastructure and new visions of a more livable community, there must be new ways to sustain cities across our planet. There must be strategies for coping with climate change and global warming. In tandem with efforts toward sustainability there must also be initiatives to relieve the congestion and density of megacities and to stem the tide of growth of urban centers and massive global population increases.

There is an organization whose slogan is ZPG (Zero Population Growth) for the World's Sake. This program's objectives have many goals related to climate change, food and nourishment, economic opportunity, education and healthcare. Yet quite separate from these goals, the vulnerability of vital electronic infrastructure that might be rendered inoperable by natural disasters or terrorist attack is truly another area of vital concern. The loss of telecommunications and networking capabilities and vital infrastructure, on which perhaps 80% of the jobs in the economically developed world now depend, represents a frightening reality. In essence, the smart city of the future must also be a secure one.

Our electronic networks are at the heart's blood of megacities with populations of over ten million. Transportation, service jobs, water and sewage, banking, food supply, army, police and fire fighters are rendered virtually helpless without telecommunications, power and networking. This is a vital fact that should not be overlooked. Vulnerabilities to natural events such as coronal mass ejections from the Sun, or disasters not tied to terrorists, must be better understood as we contemplate the future.

All IT networks are growing bigger, better, faster and more pervasive, and the scale of change is now increasing on an accelerating pace. The one dimension where there is no improvement is with respect to vulnerability and declining resilience to natural disasters or terrorist attack.

We hope the twelve strategies put forward to achieve a 21st century smart city as outlined in this final chapter will help steer a steady path forward into a better tomorrow.

Chapter 2
The Challenges of Envisioning and Planning a True Smart City

Effective urban planning is a tough slog. It requires commitment, a willingness to learn from others, and a true community sense of vision. If you thought creating an effective city government and achieving a better community was a challenge 50 years ago, there are many reasons why this is many, many times tougher today.

Despite the enormous challenges of creating a smart city that works well with strong citizen support, it now seems that everyone is trying to get into the act. Long ago, in Silicon Valley in California, both Facebook and Google-Alphabet, created work environments complete with rec rooms, waterfalls and kegs of beer to keep workers engaged and to see their offices as a second home. But today they seem poised to go a step further and to jump onto the bandwagon of creating a smart city for their employees. Some believe the timing, particularly for Facebook, is not well advised.

However, such initiatives are moving ahead apace. The Google-ABC "Alphabet City" will apparently include 5000 homes and infrastructure built in Mountain View where Google and ABC employees can live, shop, recreate, and even test out new Google products and services in their new corporate homes. The even more ambitious so-called "Zuckland" will allow Facebook employees to live, work, and exist 24/7 entirely inside their "company store."

As a friend of ours satirically quipped after reading about the "weaponization" of social media by Cambridge Analytica and Facebook's role in making this happen, "What could possibly go wrong with a Facebook-designed city and agreeing to live in Zuckland?"

As the story in the *New York Times* about the plans for these new Silicon Valley-based smart cities observed, maybe this made a good deal of sense: "After all, it is much harder to find a place to live in Silicon Valley than a new job."[1] Our vision is much broader than that of a company town. The vision is more expansive and the challenges are more profound than building a high-tech company town, where everyone works for the local coal mine as in the classic song "16 tons" by Tennessee

[1] David Streitfeld, "Welcome to Zuckland" *New York Times*, March 25, 2018. Business pp. 1, 6–7.

© Springer International Publishing AG, part of Springer Nature 2019

J. N. Pelton, I. B. Singh, *Smart Cities of Today and Tomorrow*,
https://doi.org/10.1007/978-3-319-95822-4_2

Ernie Ford. In this modern planned company town the problem might not be "going deeper in debt" but losing one's soul to an all-consuming corporate environment.

Let's just name a few of the really big challenges—mushrooming urban populations, housing shortages and ballooning costs of home ownership, overloaded transportation systems, technology-enabled criminal behavior, rapid technological change, and the latest complications of living in an Internet world with associated stresses on democratic processes. And this does not include other banes such as super-automation, with its impact on jobs and the need for life-long job retraining, and even techno-terrorism. The challenge of our times is to keep up with the accelerated pace of social, cultural, economic, and technical change that impacts virtually every aspect of our lives. The challenge throughout the world is to keep up with the riot of technological innovation. Nowhere is this more true than in today's cities, especially megacities with populations exceeding ten million. There are today some thirty megacities that are significantly larger than many of the world's countries. These are cities with multi-billion dollar budgets and with a much longer list of difficult challenges to face that many nations faced a half century ago. Creating a smart city is truly a very, very, very big problem. We hope some of the ideas and concepts in this book can explain these challenges with some new insights and some suggested new tools.

Creating a modern 21st century smart city requires facing up to and solving a myriad of problems. We cannot really overstate the case. In truth it is increasingly challenging to plan, constantly improve, and sustain a smart city.

Urban problems and challenges are growing in size, and the degree of difficulty is increasing almost exponentially. These challenges are so enormous that they are not readily prone to rapid resolution.[2]

The authors of this book in another work entitled *Future Cities* stated a decade ago: "A 'smart city' is one that ultimately delivers enhanced public services, a better environment, business and job growth, expanded foreign investment and public safety. Successful "smart city" implementation that can also be called a "future city" or "intelligent community" requires both a well thought out business model and public-private partnership."[3] These are large challenges to meet, and it starts with an effective planning process.

The following nine "big" challenges requiring improved planning and implementation, as listed below, impact virtually all of the large cities around the world. This does not represent a comprehensive list of urban challenges, but these are perhaps the most difficult, challenging and essential urban planning sectors. Of course, this is not to say that all cities and the challenges they face are the same.

Indeed some aging industrial cities are facing a shrinking population or a declining tax base—or both. Others have a problem with endemic criminal behavior and

[2] Joseph N. Pelton, "The Rise of Telecities: Decentralizing the Global Society" in "*Thinking Creatively in Turbulent Times*," (edited by Howard Didsbury, Jr.) (2004) World Future Society, Bethesda, Maryland.

[3] Joseph N. Pelton and Indu Singh (editors), Future Cities (2009) Intelligent Community Forum, New York.

political corruption. The challenges below, however, are particularly true for giant megacities. These challenges are common to both those in the so-called developing "Global South" countries as well as those in the "Global North." These are critical challenges that the political and economic leadership of most major cities will face due to major shifts in the needs of the citizenry, population and demographic shifts, environmental concerns, employment shifts, technological change and networking, information and communication technology (ICT) trends that extend across our planet today. Let's quickly explore each of these nine critical areas.

Massive Global Urbanization

There are today some 30 megacities (i.e., cities of more than ten million people), and that number continues to swell. Some of these megacities, faced with ultra-fast expansion, typically find this rapid demographic shift taxes the ability of these cities to deliver effective services and create needed infrastructure. Cities such as Lagos, Nigeria, has seen annual growth rates as high as 6% per annum and others in India, China and elsewhere that are growing at a rate that is often as high 2–4%. For the first time in history there are more people living in cities (some 53%) than live outside the city (some 47%). Projections are that by 2050 the world will be perhaps 75% urban, or perhaps even more so. Rural populations will have shrunk to less than a quarter of all humanity. Today's urban population is now very close to four billion. By 2050 it will likely be 6.75 billion or greater. The number of new schools, hospitals, water and sewage treatment plants, highways, rail systems, airports, energy systems, telecom and IT networks this implies for cities is staggering. Furthermore the greatest growth will be in developing countries of the Global South, where large cities are already not able to keep up adequately with the demand for new infrastructure.

Table 2.1 below provides a sense of the enormous struggle that megacities will have to cope with, with the gigantic populations that can be expected by 2050. If these projections are anywhere close to correct, the 15 megacities listed in this table will each be larger than all but the largest countries around the world today. These metropolitan expanses with populations ranging from 20 to 75 million people will become virtual urban countries on their own. Planning for their needs in order to effect change to remain livable, economically and environmentally viable, safe and smart is a gargantuan task.

The bottom line is that only the megacities of the world that engage in rigorous planning to become what might be called a smart city—and do it now—will likely have any chance to succeed. In fact, even now it may still be too late to start.

By 2050 the number of cities of over ten million could exceed well over fifty. They will ring the world. This rise in megacities will be in part due to the growth of families and childbirth, but the prime source of growth will be the constant migration from rural areas and poorer countries into cities in search of jobs and higher incomes.

Table 2.1 The projected growth of some of the world's megacities by 2050

Population in millions for 15 selected megacities 1950 Projected through 2050 (Based on U. N. Figures and Extrapolation of Growth)					
Greater City Area	1950	1975	2000	2015	2050
Beijing, China	3.6	5.8	7.5	9.5	20
Cairo, Egypt	2.3	6.0	10.2	12.5	25
Dakha, Bangladesh	0.6	2.1	10.0	16.5	35
Delhi, India	1.1	4.5	12.2	18.0	40
DJarkata, Indonesia	1.2	4.8	11.0	16.2	35
Greater Area around Guangzhou, China	7.7	16	25	42	75
Johannesburg, South Africa	2.0	4.5	7.6	10	21
Karachi, Pakistan	0.7	4.0	9.6	15.0	32
Kolkata, India	4.5	7.6	12.8	16.5	35
Lagos, Nigeria	0.55	2.0	8.0	16.0	40
Mexico City, Mexico	2.8	7.0	17.8	21.5	43
Mumbai, India	2.5	6.5	16.0	22.0	45
Sao Paulo, Brazil	2.2	9.5	16.8	20.2	41
Shanghai, China	5.0	6.8	12.6	17.0	32
Tokyo-Yokohama, Japan	9.0	13.5	18.5	24.0	40

Weaning Ourselves from Carbon-Based Energy Systems

Oil and coal reserves are either being depleted or will become uneconomical within the next two decades**.**, especially in the case of coal. This is leading to the need for substantial new investments in cleaner and more sustainable energy sources such as photovoltaic systems, geothermal, wind farms, or newer hydroelectric technology such as micro-generators in urban streams and rivers. This switch makes sense even without thinking about the environment and climate change. These are systems that can supply energy for eons if we engineer them wisely. In addition there is intensive research into the design of improved and longer lasting battery and energy storage systems.

The cost of this conversion is substantial, but the key is to start to think longer term. We need to make these systems last longer and be more efficient. It is possible to engineer green energy systems that can generate energy with reasonable efficiency for 30, 40 or even 50 years. We can make them more efficient by designing better wind turbines and creating better solar energy systems such as those that use quantum dot solar cells. If the life cycles of these new systems can be extended significantly they can become more cost effective over "dirty" coal and oil-based systems based largely on their longer life cycles and "free" energy systems.

Facing the Particular Challenges on Coastal Cities

Coastal cities, due to global climate change, face enormous and quite challenging problems. These include more flooding and violent storms. Thus there is a need to build new sea walls, cede some low-lying areas to the sea, or create entirely new tunnel or bridge systems. In addition there is also a need to develop and enforce new construction standards, design and build improved electrical grid systems that are able to provide better protection and withstand the force of more energetic hurricanes and typhoons, etc. The devastating recent hurricanes and fires in the United States have caused hundreds of billions of dollars' worth of damage. These losses, incurred in Houston, Texas, Puerto Rico and the American Virgin Islands, and in California have finally impacted the thinking of insurance companies, legislators and emergency administrators not only in the United States but around the world. For each degree Celsius the average temperature of the oceans also rise, peat fields in Siberia melt, and so on. The cost of adapting to climate change will be reckoned in the tens of billions of dollars.

New Educational and Healthcare Facilities and Associated Staffing Needs

A megacity that grows by something such as 3% per annum, and thus annually adds 300,000 new residents, faces staggering challenges. Such a population increase results in a staggering impact in term of new needs for infrastructure to be built and new services to fulfill. There would likely be a need for a huge number of additional schools to serve burgeoning school age populations. There might be perhaps 100,000 or more children seeking schooling. This translates into the equivalent of adding each year over 1000 new instructional facilities capable of accommodating 100 schoolchildren, plus teachers and staff. There would also be a need for a gigantic number of new hospitals and healthcare centers capable of serving thousands of new patients. And even if these physical assets could be added there would also be the associated need for tens of thousands of additional qualified teachers and doctors and nurses.

Indeed the infrastructure of a megacity that grew by this amount would be stretched to its limits in just a few years in almost every dimension. Lagos, Nigeria, is a dramatic example of a megacity stretched to his limits by too rapid growth. These unmet needs manifest themselves regardless of whether electric power, streets and highways, telecommunications and networking systems, housing, water and sewage systems were taken into account. This might be especially witnessed in terms of a lack of qualified firemen, police, and emergency services. And on top of these shortages, there is the great probability that political officials might see a rising demand to political action to somehow provide for the reasonable employment for this now burgeoning population growth. The combination of normal endemic

growth from residents having children when mixed with the unrelenting movement of rural populations to urban centers is what creates the unique urban growth problems that represent a fundamental shift from the demographics of the past.[4]

Rapid Changes in Employment Opportunities in the Face of Super Automation

New technology, automation of many jobs, changes in demographics, etc., will come together to cause major disruptions in the employment patterns in most cities. This will be especially true for the very largest cities. Unemployment and creation of new jobs coupled with patterns of employment and massive re-training of workers will perhaps be one of the greatest challenges for urban planners and the political leadership. This will make new and effective public-private partnerships even more important.

Many people think of automation in the form of putting robots to work on assembly lines. Super-automation covers a much broader range of jobs. In the most economically developed countries, such as the OECD countries, roughly 80% of the jobs today are so-called service jobs. It is those jobs that are now being replaced by smart machines. Check-out machines in grocery stores and hardware stores and automated gas pumps are already familiar sights in many countries. The next phase will involve more sophisticated machines with "expert systems" logic, artificial intelligence and sophisticated algorithms that can increasingly perform the tasks of property assessors, sales clerks, truck drivers and even airline pilots. When the IBM Watson system can be configured not only to win at "Jeopardy" but also to become so well-informed that the world's best doctors and diagnosticians sense the rate of change, automation in the world of employment is going into overdrive.

The already cited study by McKinsey and Company that projected 70 million people will see their jobs be replaced by machines in the U. S. work force by 2030 is unlike the Industrial Revolution. In the United States about seven million people moved from farming and mining to manufacturing over 70 years or so. This was about one million people per decade. Today we are anticipating something like 70 million people in one country losing their jobs in 13 years. This means over five million people a year. The rate of transition works out to be some 50 times more intense. The bottom line is that retraining and creation of new jobs in the city will never be able to keep up. Massive employment concerns will result even with greatly expanded retraining programs. This could be the number one problem in the smart city because of the consequent impacts that will come from technological unemployment and the ever greater embrace of super-automation techniques.[5]

---

[4] Joseph N. Pelton and Indu Singh, *The Safe City: Living Free in a Dangerous World* (2013) Emerald Planet, Washington, D.C.

[5] Joseph N. Pelton and Peter Marshall, "MegaCrunch: Ten Survival Strategies for 21st Century Challenges", (2010) PM Associates, London, U.K.

Changing Demographics, Aging Facilities and Inadequate Urban Infrastructure

In most budgeting processes within cities, there is a tendency to consider the top priority to be responses to growth and the launching of new programs. Maintenance and replacement of aging infrastructure such as water mains, highway overpasses, and old bridges are generally delayed until "next year" or even "next decade." The smart city planners must consider the new and better, but also face the real needs of maintenance, repair, and replacement of old and tired infrastructure.

Poverty, Overcrowding and Lack of Housing

These issues are hardly new. Cities have been faced with such issues for centuries. Smart cities need to face these issues in more intelligent ways. The relocation of rural populations to cities at an ever increasing rate plus the problems of unemployment and underemployment that accompanies super-automation that now impacts farming, mining, manufacturing, and more and more service jobs, has accelerated the impact of these problems. Here systemic solutions must be sought with new smart approaches and solutions. This will mean things such as new tax incentives to provide rewards for smaller families. It will also create the need for meta-cities that surround megacities to relieve overcrowding and allow relief of super density problems.

Coping with Terrorism and Cyber-Assaults on Automated Urban Systems

The response to many of these key urban challenges will be to create smart and automated infrastructure and intelligent systems that can provide key services more efficiently and at lower cost. Yet these new and more efficient automated systems can only be effective if they can be protected against attack by cyber-criminals and techno-terrorists. These strategies to protect smart urban infrastructure and services are the main thrust of this book.

Coping with the Megatrends That Threaten to Overwhelm Cities Globally

There are essentially two ways to face all of the above key threats and challenges. One way is to attack these issues one at a time-piece-by-piece as if they are unrelated. The other is in a more systemic way that sees many of these issues as being

interrelated and interdisciplinary in nature. Cities should seek to reduce growth to 1% or even steady state populations while finding ways to boost productivity and economic growth consistent with the needs of employment and broadened prosperity.

The possibilities are diverse and need to be tailored to the needs and interests of the countries and cities that are impacted. Most approaches involve a combination of technology (involving such things as birth control systems, modernized infrastructure, and new ways to deliver services), taxation systems and incentives, or financial or political policy.

Examples of policies that could be adopted are numerous, longer-term and shorter-term, sometimes highly inventive and possibly counterintuitive and even seemingly contradictory. In short there is no silver bullet that provides a universal solution for all countries and all jurisdictions. In some jurisdictions there might be attempts to moderate population growth involving controversial measures such as tax policies in Singapore and other countries. These have reduced or eliminated tax deductions for children. Various taxation and financial measures, for instance, could be used to incentivize smaller families, lead to fewer births and/or encourage a more steady state population. In China governmental policies have encouraged delays in the date of marriage to limit procreation.[6]

Other steps might be taken to use increased taxation related to the automation of manufacturing and service jobs in order to compensate for reduction in jobs and to generate funds for job retraining. There are numerous studies about ways for urban planners to cope with increasing rates of urbanization, significant population growth, climate change, super automation, and use of financial and taxation tools to cope with some of the above challenges. It is recommended that these various studies be reviewed and studied by urban planners. In short this is beyond the scope of this book to address such concepts in any detail. Referenced documents are only a few of those available on this topic.[7]

Our focus in this book is thus on how to create a smart planning and implementation process. In short the emphasis here is more on envisioning, strategic planning, process, and integration of the five steps that we see as crucial to effective urban planning in the 21st century. Follow these steps, as outlined below, if you wish to know how to create a modern 21st century smart city.

---

[6] Ibid.

[7] Joseph N. Pelton and Indu Singh, *The Safe City: Living Free in a Dangerous* World (2013) Emerald Planet, Washington, D.C. Also see: Joseph N. Pelton and Peter Marshall, MegaCrunch: Ten Survival Strategies for 21st Century Challenges, (2010) PM Associates, London. Also see: Joseph N. Pelton and Indu Singh, editors. *Future Cities* (2009) Intelligent Community Forum, New York.

The Key Components Needed to Create and Sustain a Smart City

This chapter addresses the key building blocks that one must effectively utilize to create a true modern smart city that is responsive to the needs of its citizenry and its business community as well as their aspirations for the future. The key elements as depicted in the chart below will be addressed in detail along with an explanation as to how these key components build on one another. This book primarily focuses on the basic objective of urban security, but the other aspects, such as a vision for the future and clear goals to aspire toward, a dynamic and responsive urban planning process, the effective and responsive use of technology and standards, and the creation of effective infrastructure that can build a sustainable community must all mesh with the security and disaster management systems of the smart city. Without the integration of all these components the community will ultimately fail. This book indicates a clear pathway to success in creating a community that is not only smart but cohesive, sustainable, and designed to be successful for the longer term.

The five key components are highlighted in Fig. 2.1. These are: (i) a truly long-term yet flexible and ever-evolving vision of the future for a city. This vision must have both clear objectives and widespread and continually reaffirmed citizen support for the vision's primary goals; (ii) a dynamic urban planning process that controls efforts to build toward that vision. Thus planning efforts must help to control growth, modernization, repair and maintenance for all of the city's key infrastructure, plus

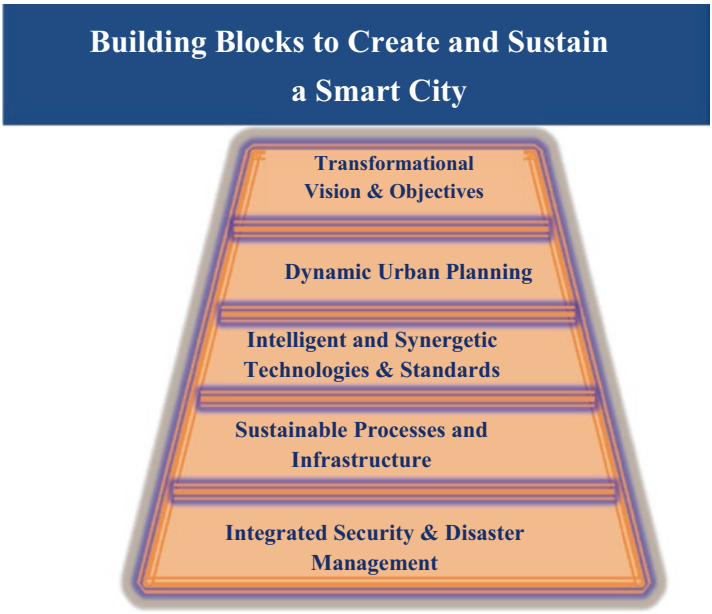

Fig. 2.1 The critical elements of a smart city in the 21st century. (Graphic by the authors)

the scope and quality of city services. It must adapt that vision to real programs and budgets based on the city's finances, taxation revenues, employment trends and ever important community security measures (i.e., from first responders to cybersecurity); (iii) intelligent and synergistic technologies, systems, and standards; (iv) sustainable processes and a reliable and responsive infrastructure; and (v) integrated security and disaster management that protects a city against catastrophic natural disaster and responds effectively when events do occur, provides effective first responders to address community needs, and ensures that vital infrastructure is secure against criminal cyber-attacks and techno-terrorists. All components must work effectively, seamlessly, and in concert with the primary vision for the city. Without these elements working together we do not believe a city can be smart nor viable in the longer term. Let's examine the components one at a time.

Transformational Vision and Strategy

Most megacities around the world must cope with urban sprawl and the bane of massive traffic jams at their central core. Crime, congestion, and pollution can also come with overpopulation and excessive and too rapid growth.

Runaway population growth of a city and accompanying urban sprawl is bad for a city and particularly for megacities. There must be a new vision for megacities that goes beyond amoeba-like spread across the landscape. In the beginning urban density has its advantages that come from effective mass transport and economies of scale. This is good for smaller scale cities, but super urban density that creates too much crowding and slums becomes bad again. Thus there is a need for a transformational vision—especially for the very largest cities.

The key to the future is to develop mid-tier satellite cities that are secure, can offer new job opportunities, environmental sustainability and use technology to create a healthier new urban environment. Pilot projects are based on the good—and bad—experiences derived from Reston, Virginia, and Columbia, Maryland, etc., in the United States, from Milton Keynes in the United Kingdom, and so on. These new paradigms that are essentially tele-city extensions of very large cities can help define both the "vision" and prototypes of the cities of tomorrow. Some of these pilots can even be created within the larger city as a restoration and revitalization process. Here there are many examples, including the 40-year remake of the so-called "Shirlington Village" in Arlington, Virginia. Vision in the abstract without viable prototypes and pilot projects can lead to dead ends and even disastrous results. Within this five-step smart planning process much can be accomplished.

Currently Planet Defense and its partner Data Mi, are seeking to develop a systematic way for urban planners to engage in urban planning across many sectors and to see how they interact. This type of multi-variable trade-off exercise in urban planning has of course been done before in the popular computer game "Sim City" but not in a way that allows one to use real data

input and manipulate what we call smart data so that outcomes can be clearly projected. This planning tool seeks to explore not only shorter term but longer term results. It also seeks to examine the degree to which there is flexibility to change various infrastructure pieces and educational and health care systems over time as demographics and other key elements of a city's makeup evolve and change over time. In the smart city, flexibility, adaptability, and updatability are all considered key virtues for both dynamic urban planning and "visioning" when seeking to define key goals.

And where will smart cities be built? The answer, of course, is everywhere. A smart city is not dependent on location but on a state of mind. Well established cities that are centuries old can re-invent themselves. New cities can be created from scratch, although a large number will emerge as suburbs or exoburbs of large, well established cities that provide, for instance, key cultural (i.e., art museums and performance centers), financial (i.e., stock and commodity exchanges), social and entertainment (i.e., sporting arena), and transportation facilities (i.e., airports and transit systems). In short smart cities have already emerged and will continue to be designed and created all over the world in both developed and developing countries. These smart cities will often emerge as retrofits within urban cores within well-established super megacities, along with new meta-cities, and also transform existing medium-sized and smaller cities as well.

What does it take to create a smart city? It is really not the new technology, robotics, expert systems, intelligent software or AI heuristics and algorithms. No, most of all it involves the ideas, visions and commitment of people. Thus a smart city requires most of all what President George Herbert Bush called "the vision thing." And that is just the start. It also requires the political, governmental, civic and business leaders who have the drive, ambition, and urban planning skills to set the wheels of progress in motion.

No one has to start from scratch. There are examples out there—both good and bad. The best examples and the worst provide useful learning experiences. International partnerships are quite helpful at all stages from planning, designing, evaluating alternatives, financing, building, equipping, and ensuring its security. There are many approaches that can be taken, but the most efficient approach might be to plan to create what we call new meta-cities. These on the outskirts of megacities can provide relief from the super density of urban cores that have too many residents, potentially failing infrastructure and significant financial, employment and other problems in terms of transportation, energy, water and sewage systems. If conceived well and designed and built well, meta-cities can provide relief to megacities that have exceeded their optimum size. Our motto is that urban density is good and suburban sprawl is bad, but urban super-density that exceeds the point of diminishing returns can and is bad again. These issues will be returned to in the chapters that follow.

Dynamic Urban Planning

Translating vision and long-term goals into effective yet dynamic urban planning is not easy. Part of the planning process is to convert vision into workable master plans that cover zoning and building standards, housing, transportation, information and communications technologies (ICT), education and healthcare, and other key areas. Many communities are now adopting master energy plans that are closely aligned with environmental standards and control of air pollution in order to reduce carbon footprints.

Some of the key elements used in urban planning today involve interdisciplinary thinking that explores how driverless cars can impact highway construction, or how telecommuting and "hoteling" within office buildings can impact the need for constructing additional office space. Likewise tele-health systems and tele-education can affect the need for new clinics or schools. Other new ideas such as ancillary dwelling units can accommodate the need for new or lower cost housing.

Integrated projects are also another aspect of smart city planning. Thus, in some cities, schools and local governments have created consolidated warehouses, recycled schools into senior centers or arts centers and engaged in joint procurements of equipment, buses and trucks. They have also found creative ways to combine facilities. In Arlington County, for instance, the nationally noted Signature Theater has found a way to build three different auditoria together with the latest Shirlington Public Library. They have also created new parkland and recreation facilities at the other end of the Crystal City development tract. None of these smart city activities or decisions involved technology but rather entailed smart planning. One of the keys to smart master plans is the ability to update, adjust and refine the plans to adjust to new needs and new demographics.

Intelligent and Synergistic Technology, Systems and Standards

Just as one needs intelligent and dynamic planning, there is a need to apply technology, systems and standards in a flexible and forward-looking way as the next step in the process. There is often a tendency to focus primarily on technology, since new smart devices are perhaps easiest to procure. New standards and systems of operating, repair, and maintenance are also of critical importance. Cities have been dependent on technology for a long time.

Mass transit systems in some cities are almost a century old. Yet repairs, maintenance, systematic upgrades and improvements over time have brought about fundamental change. The technologies associated with transportation, telecommunications, networking, and energy have perhaps undergone the most fundamental changes over the past century.

The last three decades have seen the advent of scores of key new technologies in cities across the world. These technologies have included the Internet, the Internet

of Things, 5G broadband communications, high throughput satellites, mega-LEO satellite constellations, global navigational satellite systems, photovoltaic energy systems, wind farms, plus SCADA industrial control systems for traffic light signals, pipelines, metro systems, electronic grids and transformers, elevator systems, water and sewage treatment plants and dozens of other technologies and modernized systems.

The introduction of computers, advanced, intelligent software, and digital communication systems have probably provided the greatest impetus for technological change within cities. This technology has not only led to newer and smarter physical infrastructure but changes in processes and services as well. Property and tax assessments, billings and collection of revenues, operation of transit systems, water distribution, sewage treatment plants, changing the timing increments for traffic signals and more are controlled by machines, and especially data processors. Remote sensing satellites carry out mapping and surveying functions and detect patterns of growth and development as well as detect pollution and now even help to monitor criminal behavior. Technology, new system processes, and standards are critical to most functions of modern government. These capabilities save time, money, and labor while generally adding to reliability, resiliency, and safety of operation.

We are currently at a tipping point with regard to the use of smart technology, systems and standards. Smart sensors, processors, and digital communications systems can probably operate cars, trucks, street and highway grids, rail systems, airplanes, and more with greater efficiency and safety than human operators. Yet humans are reluctant to give up control to machines regardless of what the statistical data may show. Much of this concern with regard to so-called super automation comes from a psychological fear of giving up control to machines, but the other dimension of this concern comes from a realistic understanding that machine controls can be hacked by cyber-criminals and techno-terrorists that could create widespread mayhem if they were able to reprogram machines that control vital systems. Humans may be less efficient than machines, but they generally cannot be programmed to carry out massive criminal attacks and create urban-wide disasters. The use of artificially intelligent systems within digital security systems could eventually create cybersecurity systems that would "understand" that carrying out certain commands were "wrong" and counter to public safety. A recent report from the American Institute of Aviation and Astronautics has indicated the following important trend in this regard:

> *The next generation of cybersecurity products are increasingly incorporating Artificial Intelligence (AI) and Machine Learning (ML) technologies. By training AI software on large datasets of cybersecurity, network, and even physical information, cybersecurity solutions providers aim to detect and block abnormal behavior, even if it does not exhibit a known 'signature' or pattern. Experts anticipate that, over time, companies will incorporate ML into every category of cybersecurity products.*[8]

[8] "Artificial Intelligence for Cybersecurity" American Institute of Aeronautics and Astronautics, http://www.aiaa.org/protocolAI/ Nov. 18, 2017.

This type of proven ability of cybersecurity software with smart machine learning capabilities that can avoid computer programs to carry out acts of terror are now under testing. There are those who have concerns that such a future where machines become as smart as or smarter than humans represents a truly grave danger, while others argue that AI and the so-called "Singularity" (see below) will bring enormous benefits. Mark Zuckerberg, CEO of Facebook sees enormous potential:

> *In the next five to 10 years, AI is going to deliver so many improvements to our lives…..If you're arguing against AI, then you're arguing against safer cars that aren't going to have accidents, and you're arguing against being able to better diagnose people when they are sick.*[9]

Others such as Elon Musk have foreseen a time when AI heuristic logic systems achieve "super-intelligence." This would be a time where machines have advanced beyond human-level intelligence, and this condition and time has been characterized by Ray Kurzweil as the Singularity. Musk has indicated that these super-intelligent machines may end up having goals and objectives not in-line with their creators.[10]

What is not widely recognized is that today AI systems, along with Supervisory Control and Data Acquisition (SCADA) systems, are more and more already in control around many parts of the world. Pipelines are pumping millions of liters of water, gas and oil across thousands of kilometers. Largely automated aircraft on auto-pilot are involved in the automated landing of aircraft, especially in cloudy or foggy conditions. These systems rely on automated Global Navigation Satellite Systems (GNSS) and aircraft-based sensor and data processors. Self-driving cars and trucks are soon to come online along with largely automated mass transit and rail systems. People are reassured by the pilots on board the aircraft, and the train operators on board mass transit trains, but in many cases the computers are largely in charge.

Sustainable Processes and Reliable and Responsive Infrastructure

The technology, systems and standards are constantly being evaluated and upgraded to do new tasks in the 21st century smart city. The object of urban planning processes is most frequently to create infrastructure that is functionally better, safer and more reliable. There are also efforts to make this infrastructure more cost efficient and more resilient. In the case of sustainable energy systems these objectives go together. For instance, solar cell or wind farm systems that can perform without excessive maintenance costs for prolonged periods, such as 30 years or more, and with reasonable efficiency can be highly competitive in terms of cost.

---

[9] "Elon Musk and Mark Zuckerberg's Artificial Intelligence Divide: Experts Weigh In" *The Wrap*, July 25, 2017 https://www.thewrap.com/why-mark-zuckerberg-and-elon-musks-are-artificial-intelligence-adversaries-draft/.

[10] Ibid.

The next chapter addresses each of the key infrastructural elements to be found in a smart city and how adding intelligence, flexibility, and interdisciplinary capabilities to this infrastructure can help achieve the longer-term vision. This does not always mean the highest level of technology. The goal is to find ways to make infrastructure more adaptable, flexible, updatable, sustainable, cost-efficient, resilient, and capable of meeting community objectives. There is not one single formula that sets forth what infrastructure to build and install in a particular community. A good deal of smart data about how a community uses transportation, communications, IT systems, energy, water and sewage systems, waste removal, etc., plus information about where and how people work, where they go for recreation and relaxation, and how they spend their time on a 24-hour a day, 365 days a year basis is important.

Most executives would be surprised to find that they spend only about 8–10% of the 8760 hours of a calendar year in their office (i.e., 700 hours to 876 hours), and that they spend about 3% of their time (i.e., about 250 hours) either in commuting to and from work or on travel. Such analysis drives some businesses and governmental units to move toward emphasizing telecommuting. There are many similar smart data analyses that might be undertaken to reveal how to use transportation systems more effectively, optimize housing, share spectrum, or improve the efficiency of water treatment plants. The possibilities to use infrastructure more effectively, secure systems more securely, or reduce costs will be explored further in Chapter 3.

Integrated Security and Disaster Management

When different people hear the word "security" they often think of quite different things. Some first think of national defense against warfare or police protection to provide prompt response to theft, robbery and assault. Others think of potential natural disasters and protection from violent storms, flooding, earthquakes, volcanic eruptions. Others think of fire protection, the dangers of hazardous materials, potential attacks by biological or chemical agents, and in today's world of hacker attacks perhaps most frequently of criminal or terrorist cyber-attacks.

Smart cities must be equipped in all these ways to provide for the security of its citizenry, its businesses, governmental structure, and other institutions, as well as its vital infrastructure. It is in all of these types of security that must be considered in designing, implementing, and operating a smart city. Most cities tend to focus on first responders and having good police, fire-fighting and EMT capability and leave national defense to national armies, navies and air forces. What is more often overlooked and underfunded are defensive measures and capabilities to cope with natural and human-made disasters and cyber-defenses.

One of the steps taken to create better security is to realize how transportation and building standards are a part of the security framework. When truly inefficient buildings that are over 100 stories high are authorized and built—when safety and security are taken into consideration—there should be a smart analysis completed.

This analysis would consider such issues as what if there is a fire on the 88th floor? What if a jet airliner by terrorist intent or by accident flies into the 56th floor? What are the transportation, security, and energy implications of consolidating so many people into one such concentrated area in terms of daily commutes to and from the building, in terms of an attack or malfunction of the building's air conditioning, heating and ventilation shafts, or the heating and air conditioning energy efficiencies of such an office building.

Suburban Sprawl Is Bad, Urban Density Is Good, But Super Density Is Bad Again

Throughout this book, the theme of density being good but super density not being smart and indeed being "bad" will occur again and again. Super density creates problems with transportation, energy efficiency, infrastructure and its maintenance, and especially with personal security. "Edifice envy" in modern cities that leads to the building of super skyscrapers has not been sufficiently analyzed in terms of both terrorist attacks and natural disasters such as earthquakes, fires and other more mundane issues such as the failure of elevator systems. After the 9/11 attacks on the World Trade Center in New York City, it would have been wise for all city planners to re-evaluate the types of problems that too tall edifices can bring. Particularly in the age of broadband communications and virtual presence the wisdom of using more telecommuting systems and electronic decentralization to distribute population rather than create super density would seem not only smart but also wise from a cost and expenditure view point of view. Arthur C. Clarke, the futurist guru who predicted key inventions with amazing foresight, predicted the rise of tele-cities simply because they are so logical. However, people are motivated more by their ego and economics than by their brains. In short megacities are being created for all the wrong reasons.

Smart businesses and governments are today experimenting with "hoteling" of office space and telework systems. The County of Arlington today has workers in Minnesota and in other parts of the United States that perform telework tasks that require no visits to local offices throughout the year.

The Power of Innovative Smart City Solutions

A smart city and positive innovations can manifest itself in myriad ways. The desire to improve a city's infrastructure, its services and operational efficiency, or its economic effectiveness and employment, can be aided through many types of innovation. Just a few examples of smart city planning and innovations include the following.

Intentional Dwellings and Innovative Offices

Housing and business offices have evolved little over the past few centuries. Offices and houses are inefficiently inhabited and used during the 168 hours of a week. Some studies of executive offices indicate they are inhabited only 7% of the time in a full calendar year. New models are emerging. There are shared offices serving many clients. There are also offices that include gyms, botanical gardens, urban farms, restaurants and bars.[11] There are also new housing arrangements geared to those seeking new forms of connectedness within communal housing with small apartments that adjourn large chef kitchens, libraries, and recreation rooms that are more space and energy efficiency but also provide companionship, people with shared interest, and a way to overcome loneliness. One study has estimated that over 42 million people in the United States are suffering from what is called chronic isolation.[12]

Embracing the Strengths of the New "Hive" Mentality

Millennials with a new sense of sharing, use of social media, "hive thinking" and collaboration are more open to working online, combining business with social experience and blurring the lines between home, housing, work, play, education, recreation and communal experience. Some of these models might also be reapplied in the housing, entertainment, cultural experience and dining patterns for seniors, for college students, and professionals in consulting and other services. These new models that have emerged in Silicon Valley and New York in the United States are blossoming around the world and across America. Such trends can merge with re-development and revitalization of neighborhoods. Old churches or warehouses might, for instance, become new types of shared communal housing or offices.

Virtual Companies and Industries

There are many factors that are motivating companies to rethink the traditional model of companies, especially service companies, consolidating all of their employees in a single large office where employees commute to and from work for an 8 a.m. to 5 p.m. workday five days a week. The down sides of the traditional business logistics model are many. There is the ever rising cost of high rise space in the heart of a city, the adverse environmental effects such as greenhouse gases and

[11] Susan Dominus, "Rethinking the Work-Life Equation" New York Times Magazine, Feb. 28, 2016 https://www.nytimes.com/2016/02/28/magazine/rethinking-the-work-life-equation.html.

[12] Jeffrey Kluger, "Americans of all ages are coming together in 'intentional communities'", Time Magazine, November 27-December 4, 2017.

acid rain, to the inefficiency of workers spending so much "down time" in rush-hour traffic. On the upside of new models there is lower pollution, the efficiency of using teleworkers recruited both nationally and internationally (i.e., electronic immigrants), and the ability of a small and nimble company to have a global presence and serve global markets. Virtual companies can be more nimble, flexible, have lower overheads, aid in a cleaner environment and recruit workers from a broader base. There are productivity gains at multiple levels, although IT and telecommunications security can pose a problem.

Embracing Zero Carbon Footprint Green Urban Systems

There are hundreds of ways to go green with smart city technologies. There are smart streets that can aid traffic flow. One can telecommute to work and reduce gas emissions from cars and downsize office space requirements in buildings built for hoteling to accommodate workers who are only occasionally in the main office. One can install motion sensors to activate lights, escalators, and machines that do not have be on 24/7. One of the more important changes for new smart city developments would be to create district energy systems that save energy in a number of ways. Such new developments would of course also be designed to produce green energy via solar, wind, geothermal or other means.

Secure and Protected Human-Machine Interfaces

There are thousands of other ways to make cities smarter, more livable, and more energy efficient, but there needs to be an accompanying vigilance against cybercrime and techno-terrorism. Clearly this involves anti-viruses, firewalls, facial recognition systems and code access cautions. But the most important aspect may well be human-machine interface (HMI) processes that can shut down runaway smart infrastructure. The importance of cybersecurity systems and vigilance will only increase with the use of artificial intelligence and cyber-systems in every aspect of a smart city's operation and design.

Conclusions

Urban security involves many issues and considerations. These include building standards and zoning, training and funding of first responders, protection of homes and buildings and people against natural and human-made disasters, and increasingly cybersecurity and efforts to protect against terrorist attacks. These issues will be addressed further in later sections of this book.

The five essential elements critical to creating a smart city are noted in Fig. 2.1 earlier. These are needed to pursue the design, implementation, operation and upgrade of a smart community. All of these elements need to be combined in order to build a new urban vision for tomorrow. All five are of great import. All five components of vision, dynamic planning, smart technology and standards, sustainable processes and infrastructure, and integrated security and disaster management must be embraced and respected as essential by urban leadership. This five-step formula may sound simple, but it is difficult to implement successfully. Narrow vested interests, corrupted officials, a lack of vision and a lack of community involvement can frustrate efforts to build a better community. The elements of automation and technology associated with creation of smart cities makes security and especially cybersecurity much more important than ever before.

One of the most common problems in creating and sustaining a smart city is a lack of continuity in the political and professional leadership of a community. This can lead to a changing vision of what a city is and what its citizenry strives for it to be. Another key problem is when political or professional leadership fails to involve the community, resulting in no clear-cut, shared vision.

This lack of commitment to that vision often translates into a lack of support when it comes to funding that vision and bond issues fail or tax rates are insufficient to support modernized infrastructure. A city is quite complex, and keeping all of the moving parts working together is quite difficult. Mayor Twu of Chiayi City, China, has said: "A city is like a person. It has many systems – like how a person has a nervous system, or a cardiovascular system."[13] If the political and professional leadership of a community does not recognize this complexity and fails to pay attention to all of these systems and nurtures them, its long-term vision will of necessity fail.

The Intelligent Community Forum (ICF) in New York City has now built a database that includes the best practices of some 400 cities around the world. If one goes to their website one can find a useful definition of what they call an intelligent city. The ICF even provides a way to assess your city in terms of its intelligence. This assessment process can provide some valuable advice about how to improve your city, and perhaps most importantly, ways to connect to other smart cities and learn what has worked for them.[14]

The smartest city planners and leaders look to the experience of those who have sought to be better and found smarter ways to build their cities become stronger through a variety of means. Sometimes this is through better practices, processes and standards. Sometimes it is through better technology and software, but other times it is through better maintenance practices and interdisciplinary or interdepartmental cooperation. Learning from those that have succeeded elsewhere is always a smart practice.

---

[13] Mayor Twu, November 19, 2017 https://www.facebook.com/IntelligentCommunityForum/photos/rpp.51163322600/10154633444512601/?type=3&theater.

[14] Intelligent community forum home page, http://www.intelligentcommunity.org/ (last accessed Nov. 19, 2017).

Chapter 3
The Critical Infrastructure and Software Needed to Build a Smart City

There is no one template that one follows to create a smart city. It is just not that simple. Anyone who says that they have a straightforward and foolproof plan for you to follow to design, implement and operate a successful smart city—well that person is lying!

Many factors come into play. These factors that help differentiate different cities include at least the following: geographic location, local governmental structure, efficiency and integrity of operations and management, primary and secondary industrial and commercial base, national defense and military bases, and status of national government, cultural, ethnic and linguistic traditions, infrastructure serving the city, current and prospective standards of living, and different strata of education, health and prosperity among its citizenry.

And this is just for starters. A city's current status also strongly relates to the strength of its tax base, degree of modernization and efficiency of its key infrastructure, efficiency and automation in the public and private business sectors, efficiency and training of the workforce, and especially the degree of acceptance of the political, social and economic structure at the local and national level. Before you know where you are going and where you want to be, you must know clearly where you have been and where you currently are today. Taking stock is a very good place to begin.

Nevertheless, despite the great differences among the various cities of the world, there are common denominators that apply to any assessment of urban infrastructure and its modernization. It is possible to assess the degree to which a city has evolved toward becoming an intelligent community. There is no single arbiter that decides when a city can legitimately be deemed smart. Yet a city without key infrastructure that has been modernized and which lacks well trained and committed staff stands at a great disadvantage. If an urban center does not know how to utilize its infrastructure to best effect it is not truly smart. If a city's leadership and workforce does not continually consult with the community about the types of services desired and respond to those needs to seek improvement, it has a major liability to overcome regardless of its current status.

© Springer International Publishing AG, part of Springer Nature 2019

J. N. Pelton, I. B. Singh, *Smart Cities of Today and Tomorrow*,
https://doi.org/10.1007/978-3-319-95822-4_3

There are core infrastructure systems that all communities probably need to address if a city undertakes to be defined as being or seeking to be smart. The following key elements are fundamental to most smart communities. These elements are: (i) an effective educational, training and healthcare systems; (ii) viable transportation systems; (iii) accessible communications and IT systems; (iv) energy, power, and environmental control systems; (v) other vital public infrastructure including water, sewage, and trash disposal; and (vi) public security, including first responders, effective capabilities to respond to disasters, and, increasingly, in the past few years, cybersecurity.

In order to implement and operate these modern aspects of a smart city it is important to sustain the overall economic vitality of a city. This ongoing effort to upgrade and improve the urban infrastructure depends heavily on viable public and private employment, a committed citizenry, and a reasonably solid tax base. It also requires an ongoing and dynamic urban planning process that constantly seeks to provide fair, just and always improved governmental services. This chapter addresses all of these critical areas and explores how smart technology, systems, and processes in all of these areas can elevate urban capabilities and strengthen a city's ability to respond to public needs.

Note well that nowhere in this listing of vital infrastructure for a smart city, do we see the words "technology" or "automation." It is vision, commitment to change and an ongoing process that is at the core of becoming a smart city—not technology or automation.

Clearly updating of infrastructure so it will be more efficient, responsive and cost-effective does suggest change and imply technology. One always hopes that improved technology, automation, and the use of smarter machinery and artificial intelligence can bring about positive change for a community. Such change might be in terms of security, better services, lower costs, convenience, more community involvement or simply a better life. Yet before such steps can be taken to create a smarter city or upgrade civic infrastructure careful analysis should be undertaken.

Evaluating Merits of Possible Changes

This involves what might be smart data analysis or causal analysis to evaluate and in some cases simulate or model the impact of such change. All major changes and infrastructure innovations should be looked at against many criteria. These should include such aspects as public security, longer term reliability, responsiveness to community needs now and in the future, and overall societal and economic impacts. Automation and technologically leveraged services, for instance, can potentially have negative impacts on employment, social justice, political sustainability and community cohesion. These impacts should be considered and evaluated against smart data analysis before such changes are made and not after the fact. Automation that significantly undercuts social justice or economic viability is not smart and, indeed, could be quite harmful in the longer term.

There are a number of key questions that should be asked of every effort to improve a city's infrastructure proposed in the name of making the city smarter. Some examples of such questions include the following:

(a) Will plans for the future, and specifically new infrastructure investment, assist with helping to retain younger people and encourage them to return to the impacted community once their education is complete and they are seeking employment? What about other age groups? Will they truly benefit all sectors and demographic groups or will particular parts of the community somehow particularly feel negative impacts? Will these impacts change over time? In short, the potential negative impacts must be considered as well as the positive.
(b) Will planned investment in modernized and automated infrastructure translate into a more cohesive community that could be qualitatively or even better quantitatively measured over some reasonable period of time, such as 10–20 years? Here the world needs to be one's experimental oyster. The experience of other communities must be considered to see what has worked or failed elsewhere. It is not necessarily best to be on the "bleeding edge" of new technology and change.
(c) Can this change in infrastructure be given a scorecard over the next 10–20 years in terms of measurable benefits or possible liabilities as perceived by the community at large? Can this be rated in a quantitative way? This might be judged against the following type criteria: (i) educational or community training improvements; (ii) health and medical safety benefits; (iii) transportation improvements; (iv) communications or networking upgrades; (v) more effective energy systems; (vi) environmental improvements; (vii) public and private employment; (viii) parks, entertainment, recreation or physical education upgrades; (ix) improved housing or community services; (x) efficiency of governmental services; (xi) measurable impacts on the shorter and/or longer term cost of governmental services and levels of taxation; and (xii) increased public security and safety. It is important that someone other than the entity proposing a new infrastructure upgrade or retrofit be designated to do this evaluative research, to consult other communities and to fill out the "scorecard."
(d) Are there alternative investments, approaches, methods or technologies that would represent a better use of public funds? Is this a "bleeding edge" or proven technology or process? Are important cost savings possible if the investment is somewhat delayed or staged in its implementation?
(e) Does this change to infrastructure benefit the community at large equally or does it have selective benefits, and do these benefits or negative features change over time? If so, why do these outcomes occur, and can any negatives be mitigated? Is there a better way to approach or modify urban infrastructure to have a more equitable impact on the community?
(f) Is this new or improved infrastructure best financed, installed and operated as a public utility, a private enterprise, or possibly as a hybrid public-private partnership? Does this mix of public and/or privately installed and operated infrastructure change over time? If so for what reasons would this be the case? One does not need to assume that all urban infrastructure must be

owned, installed or operated by public agencies, even though this may sometimes be the only viable way to ensure this service is reliably provided.

These are only examples of the types of questions to consider. The key is to avoid technological improvements that are championed and pushed through for narrowly conceived and often technically focused perspectives without taking a broader view. It is also critical to have an integrated analytic model that can examine all of the moving parts of a community to see how change or investment in one sector impacts the city's overall economy, social cohesion, sustainability and resilience.

The following interactive model was developed by the DataMi Corporation of Colorado and is indicative of how such a smart data analysis of investments and infrastructure improvements impact all aspects of a community. In this model transportation and energy also includes environmental impacts.

Such smart data analysis starts with a concept similar to big data, which can process large amounts of data input. But in this case the emphasis is not on the volume, velocity or variation of data. Rather the key is to identify that particular data that is well verified and is of high value in terms of seeing what is the most impactful. This is sometimes called causal information. This is the data that is best able to measure significant change and to determine what are the most important drivers of change.

Thus smart data analysis can still be carried out using large data streams, but a particular type of data processing starts with what might be described as "initial interactive causal models of key interactions." In essence the idea is to identify things such as possible problems, potential urban infrastructure disconnects, or other areas where the model depicted in Fig. 3.1 might show patterns of stress or change that should be analyzed. Instead of starting with a tabula rasa one begins with some understanding of the potential significance on each data element or stream on each other (environmental interaction and influences). The purpose of this type of data analysis is to examine how interactive forces within these models first influence each other, how they affect each other over time and how forces of desired outcomes can be predicted with a high degree of probability based on simulations using data inputs.

These smart data tools and models, if properly developed and tested, can allow city planners to be better equipped to make public choices and understand the significance of those choices. By using smart data modeling techniques change can be marshaled in a more synergistic way to improve performance, safety or efficiency of operations. The effectiveness of smart data analysis depends on developing the most accurate tools and interactive models of change within larger systems such as the operation and growth of a city.

The models can also incorporate machine learning to give the city feedback on decisions as they are being made and how improvements and influencers can be measured for future decisions. This is not a one-time exercise but an ongoing operation to test results and forge new pathways.[1] The use of smart data analysis and causal analysis as key tools of smart urban planning is discussed in more detail in Chapter 5.

[1] DataMi LLC, Interviews with Stephan Andrade and Hans Brunner concerning "smart data" analysis for the development of "smart cities." Dec. 13–14, 2017.

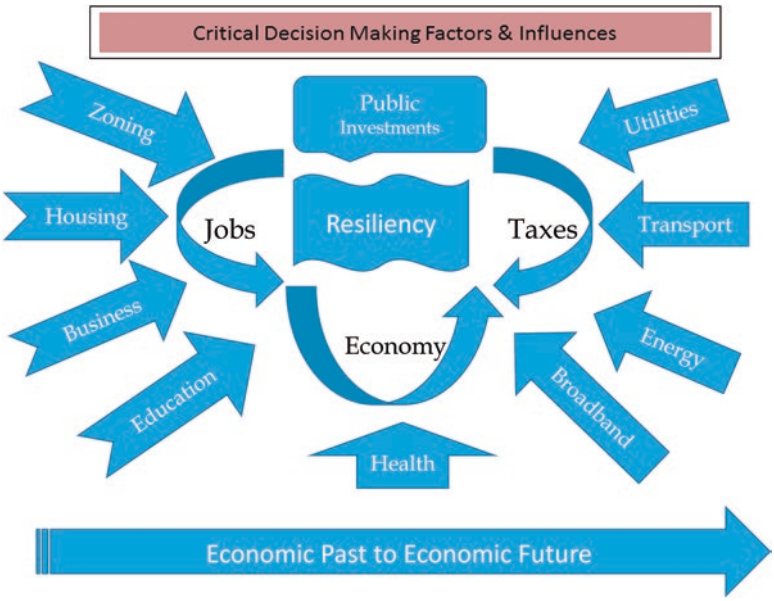

Fig. 3.1 Integrated model of urban relationships are key to undertaking smart data analysis. (Graphic courtesy of the DataMi Corporation)

Those with special knowledge of transportation, communications, networking, energy, etc., often tend to see the way forward in terms of infrastructure improvement and technological upgrades, but in a very narrow context. Sometimes they do not see the larger picture or consider all aspects of a change to key urban infrastructure and services. Most urban infrastructure upgrades and modernizations are evaluated by experts in a particular discipline about which they know a great deal. Someone that is well versed in how to plan and build roads, highways and ramp interchanges looks at traffic congestion and can tell you how much concrete you need to pour and how many houses must be cleared by right of eminent domain to build an expanded roadway. A flood control expert will tell you how much wider a storm water main must be built.

This narrow view can result in changes to a city's urban infrastructure in such a way that it leads to excessive environmental pollution, health issues, population congestion, property value surges or devaluations, or other unanticipated consequences. Robert Moses, sometimes called the Master Builder and who was consistently the advocate of building new roads, bridges and turnpikes in the New York City area, was considered to be primarily responsible for developing the sprawling development across Long Island. His automobile-focused approach to transportation, as opposed to mass transit, was key to not only the development of suburban communities in the New York City area but suburban sprawl across the United States. His dominating approach to what might be called a "car culture" made him a very polarizing figure. Clearly, he never asked these key smart city

planning-type questions about infrastructure and thus transportation infrastructure created what many consider the reverse of smart planning.[2]

Although each of the following sectors may start out being considered for upgrade and improvement, there is a need for integrated thinking about the interdisciplinary impacts on each of the above 12 sectors and possibly others. The key is thinking about the implications of infrastructure upgrades and changes in terms of how it affects the city's longer term future, the viability of the community and its responsiveness to all sectors of the community now and in the future.

The classic story about how technological fixes can go awry involves the London City Council at the turn of the 19th to the early 20th century as recorded in their minutes of the times. They were currently faced with the crushing economic burden of removing horse manure from London's streets. The council thus greeted the introduction of automobiles as an environmental and economic savior that would rescue them from bankruptcy and would provide a permanent solution to their pollution problems as well. At one phase technology can provide a solution, but at a later stage, the cure can become a new disease.

Education, Training and Healthcare Systems

The core of a smart city is a vibrant and effective system to deliver high quality educational, training and healthcare services. The key is to embrace the latest proven technologies and systems that allow these services to be delivered so as to maximize effectiveness and to contain or in some cases even lower costs. The traditional way to measure effectiveness of educational and training services is to have qualified teachers instructing in classrooms. Medical care systems have been typically seen as having a doctor examining patients, prescribing medication or performing medical treatments of one sort of another.

More recent thinking on education and training is that lecturing to students is still important, but challenging students to learn new materials and to acquire knowledge to solve problems is even more important. Challenging and motivational assignments, video laboratories, online lessons, master teachers connected to students via video links, effective interactive student activities, and improved testing procedures that allow students to advance on an accelerated basis are tools that can facilitate learning. If educational and training programs are properly organized and independently assessed, the longer term impact can even reduce costs while also improving the overall quality of the education and training. Today, these objectives can, in part, be achieved by creating Smart Schools and Smart Learning Centers.

There is no doubt that technology and devices and advanced communication and information networks are critical to advancements in transportation, communications, healthcare and improved public services. Driverless cars, pilotless aircraft

[2] Robert A. Caro, "Annals of Power," *The New Yorker* (July 22, 1974). Also see for an alternative view. Lopate, Phillip (March 13, 2007). "Rethinking Robert Moses." *Metropolis Magazine.*

(except for emergency landings), and Maglev and hyperloop rapid transport systems are just some of the key transportation systems now being developed or planned. Broadband communications and networking systems for both wired (i.e., fiber optic cable systems and coaxial cable) and wireless (i.e., high throughput satellite systems and broadband 5G—and in time 6G—mobile communications systems) services continue to offer higher and higher throughput and more and more advanced applications to aid work productivity. Blockchain systems hold significant promise for providing secured databases and protected sharing of information in the smart city architecture. The effective use of communications and networking technology and better educational and training software can allow more flexible delivery of governmental services and especially increase the effectiveness and efficiency of educational and training systems.

It is important to note that schools and training centers do more than simply impart knowledge. Schools, in most economically developed countries, serve a multitude of functions. These functions include child care for working families, a place for socialization and the learning about social norms and mores, development of leadership, social conversation and sharing skills, as well as learning such diverse things as computer and typing skills, cooking, driving a vehicle, dating, and ongoing community interactions.

The broadband networking systems to support tele-health and tele-education services can also support a multitude of other governmental services. In the case of the Arlington County, Virginia, in the United States, for instance, the so-called "Connect Arlington" system was designed to support health, education and training services and to connect over 50 sites for this purpose. The fiber network that included nearly 900 fiber links with a potential of over a terabit per second transmission throughput capability can also be used for a growing list of other functions. These functions include commands to traffic signals to regulate effectively daily traffic flows or aid emergency evacuations, create emergency hot spots at traffic accidents or, even more vitally, create a broadband wireless wi-fi system at the location of any nearaby terrorist attack.

This Connect Arlington fiber optic network can also be used to connect the local state of the art emergency 911 center to other nearby communities and various national emergency centers. One of the newest features is to use the network to link together sensors capable of detecting dangerous gases and possibly even biohazards. These sensors are strategically located at the tops of buildings and at other key locations across sections of Arlington. The sensors are networked together so they can even predict the direction and rate of flow based on wind sensor readings. This Connect Arlington network can thus support the field operations of dozens of governmental services.

Additional keys to the planning of the smart broadband Arlington system were:

(i) to create a ringed system so that a single failure did not make the system fail and go offline as well as to have emergency backup generators in the case of power failures;
(ii) to design this broadband system with flexibility so that it can support county-wide fiber optic transmission but also to allow it to provide backhaul for

connection of the various towers that are used to deploy an emergency broadband wireless network;

(iii) to envision a system that supported a wide range of health, education, and other local governmental services, but also equip it with the capability to support the communications and IT needs of private industry and even federal governmental agencies that are concentrated in Arlington County. Reliable broadband systems are critical in this area, since Arlington County currently houses Reagan National Airport, the Pentagon, the U. S. Navy Annex facilities, the Defense Advanced Projects Agency, the National Science Foundation, State Department training facilities, Fort Myers, and many other U. S. federal facilities.

The bottom line here is that many governments end up with stovepiped planning. This lack of consultation across all departments and non-coordination of programs across all aspects of urban government creates overlap, inefficiency and waste. Further the city services and systems that are ultimately offered often do not fully respond to citizen needs.

The results can be redundant communications and IT networks that only serve one purpose for one agency or one function. It is common in many cities not to have interactive planning to leverage the infrastructure to maximum advantage for government efficiency, the citizenry, and the local business community and perhaps many others as well. This maxim to coordinate key programs and the planning and operation of key infrastructure applies to energy and environmental systems, to transportation networks, to communications and IT networks, and indeed to most other urban infrastructure as well.

Innovations in health, training and education today are, in fact, more about software than hardware. Both software and hardware must be coordinated and planned. The best software can motivate students to learn, trainees to command a skill faster, and aid medical and health-related practices in an ever-expanding range of ways. One must be careful to avoid the trap of thinking that one size fits all. Language, culture, social conventions, and even religion can get in the way of learning and the best health practices and forms of medical care.

Before one buys into the use of a particular software designed to spur learning, education, or health-related practices, one should consider trials to test to see how well the software actually works in a particular community or group that is seeking to apply that particular software. Once one finds the best hardware and software the key is to see how it might be shared and used in other parts of the government. Too often there are barriers to effective communications, cooperation and infrastructure sharing between and among schools, hospitals and clinics, transportation departments, energy suppliers, communications and network providers, and other parts of government. Rather than seeing themselves on the same team, governmental units can often see themselves as competitors for sparse resources.

Further, finding the right hardware and software are only a part of the puzzle. There is still a need for onsite instructors, medical advisors and technical experts to clear up areas of confusion and respond to questions. Systems such as the IBM

Watson for medical diagnosis are truly prodigious in their capabilities, but a nurse or doctor can still be needed to convert software-based input to the desired practical output. A satellite-based or Internet-based educational program needs onsite instructors to respond to local questions and make sure all students are in a classroom or lab and getting the information required.[3]

The historical problems with such things as tele-education usage can provide a new perspective. In the case of El Salvador an effective tele-education program linked to competent teachers was started in the late 1960s and into the 1970s with funding from the U. S. Agency for International Development. The students produced by this educational program graduated and sought jobs suitable to their newly acquired skills. There were, however, no appropriate jobs available, and the result was ultimately a civil war. In 1979 there was a conflict between the military-led government of El Salvador and the Farabundo Martí National Liberation Front (FMLN). This was a coalition of several groups seeking change and demanding a new direction in the government and modernization of the company. The conclusion is that one must envision not only new and improved education systems with improved facilities and software but also a society that anticipates the needs that emerge from better education.[4]

Another example of how to choose instructional software for a community come from the so-called SITE experiments carried on in India using the NASA ATS-6 satellites to provide education and training in rural India. In this case there was an educational film that showed how house flies carried germs and viruses that caused diseases. This film showed extreme close ups of the flies and warned about the many diseases they could carry. At the end of the film the villagers that had seen the film were quite impressed with the message but said: "Fortunately we do not have these giant foot-long flies in our village." The local instructors had to carefully explain that no such flies were indeed in their village and that close-up filming of house flies had distorted the size of the health hazards they had been warned against. Local instructors have to answer student questions and interpret software to students, or even the most sophisticated health and educational software can fail.[5]

Transportation Systems and Infrastructure

As important as new, advanced vehicular and people-moving devices are, it is key to look at entire planning and control systems. In short, transportation is much more than automotive, transport and delivery devices. Today we have various forms of people movers such as elevators and escalators, trains, light rail, and metro systems, Maglev trains, aircraft, drones, UAVs, high altitude platform systems, electrical ion

[3] Empowering Heroes, Transforming Health. https://www.ibm.com/watson/health/.

[4] "Salvadoran Civil War" https://en.wikipedia.org/wiki/Salvadoran_Civil_War.

[5] Discussions with Robert Fillip, Fulbright research on the SITE experiments in India involving the NASA ATS-6 Satellite.

thrusters, spaceplanes and perhaps soon hyperloop systems, hypersonic rocket systems to move from point A to point A on Earth, space elevators and tethers to lift things to geosynchronous orbit, and mass-drivers and gravity-assist systems that can move objects, products and people around in space. Transportation systems are thus more than various types of devices that propel people, animals, produce, products, and things. There are also roadways, freeways, smart toll systems geared to times of day, railways, airports and launch pads and airborne launching systems such as Vulcan Industries Stratolaunch or SpaceX's White Knight carrier aircraft to send spaceplanes aloft. It is these various types of transportation infrastructure that often are most critical in achieving a smart approach to urban planning and innovation.

It was a new type of elevator design that allowed relaying lift cabs from one cable system to another in the building of the Burj KhalifaTower in Dubai. This buildings' remarkable new type of elevator system design allows people to reach the very top of this building in only 35 seconds and to travel at speeds as high as 40 or 65 km per hour.

This innovation in cabling systems that allowed credible ways to reach the top of the Burj Tower (nearly 700 m, or a third of a mile high) via new elevator technology is an engineering marvel. Yet as impressive as these new elevator designs actually are, the "What if?" questions remain. The building of a tower so high does not include consideration of what happens in the case of fire on the 120th floor or how people can cope in the event the elevator or ventilation system fails. It is important to consider the overall risks and downsides of new technological capabilities when a technological breakthrough makes something new possible. This is especially the case with urban planning and new transportation capabilities.[6]

A broader issue is design of street and freeway systems that create wider conduits into the center of large cities that grow ever denser in the center of the target of concentric circles. World Bank urban planner Pedro Ortiz has suggested that large cities need to develop transportation systems that are more like the layout of a chess board than a series of multi-lane freeways that funnel more and more people into the center of a dartboard target. (See Fig. 3.2.)[7]

This change in the perspective on transportation systems, both in terms of horizontal street networks, but also verticality in terms of limited density, building density and heights can impact many other aspects of a city, such as its ability to respond to fires, natural disasters, terrorist attacks, traffic jams, patterns of crime, health and medical care, education, water runoff from rainstorms, sewage requirements and much more.[8]

There are also key processes, standards, and management systems that can be vital to success when it comes to transportation. And it is important to make sure that resources are available to be spent on maintenance, repair, and network upgrades.

---

[6] TAG Archives: Burj Khalifa, March 4, 2014 http://www.elevatordesigninfo.com/tag/burj-khalifa (last accessed on December 15, 2017).

[7] Pedro Ortiz, "How to Respond to Uncontrolled Metropolitan International Growth," Bank for Reconstruction and Development (IBRD), November 2011.

[8] Pedro Ortiz, *The Art of Shaping the Metropolis,* (2013) McGraw Hill, New York.

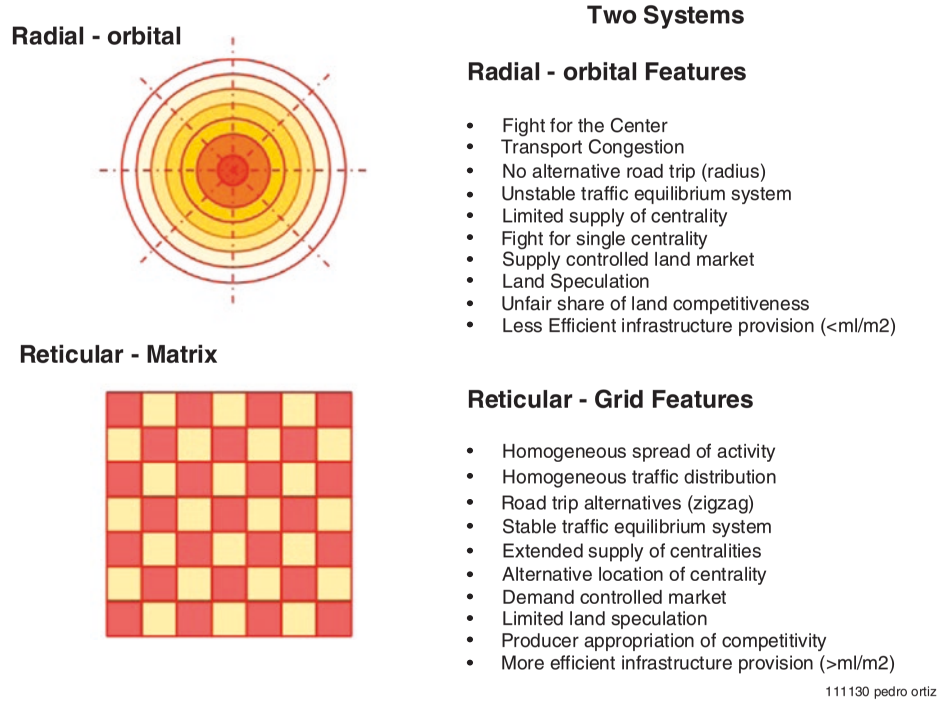

Fig. 3.2 Analysis of how transportation architecture impacts patterns of development and other urban infrastructure development. (Graphic courtesy of Pedro Ortiz)

Management and operation of transportation, energy, and telecommunications and networking systems without adequate provision for maintenance, repair and system upgrade can be deadly to urban services in this regard. In New York City, the subway system has been officially declared by Governor Cuomo to be in a state of emergency due to a failing transit system that has suffered decades of inadequate repair and maintenance.[9] The Washington, D. C., metro system has likewise fallen into disrepair, which has led to service outages and dangerous fires. This is not only a matter of inadequate maintenance but is an artifact of its unique funding and management process that derives from so many different local, state and federal jurisdictions.[10]

And these maintenance, repair and modernization concerns are in no way unique to transportation systems. There are parallel concerns with regard to all types of vital infrastructure, whether it might be concerns with water mains, water and sewer treatment plants, energy generation, transmission, pipelines, or even communications and networking systems.

The significant challenge related to transportation system decisions is that options and locations for streets and highway systems, mass transit routes and stops, and the airports of major cities can become critical in a variety of ways. Key transportation systems tend to drive economic development patterns, zoning, population concentrations, and trigger other large-scale infrastructure investments. Trains, metro systems, airports and aircraft, and the emerging technologies such as Maglev trains, hyperloop systems, hypersonic space planes, etc., can involve the expenditure of billions of dollars and lock in urban development decisions lasting decades or even centuries into the future.[11]

The layout of transportation systems for cities for centuries involved pedestrian pathways and passageways for horses and beasts of burden. This limited cities to about 5-km walkways to the extremes of the city. What followed has been a progression of new transportation capabilities. This has included trains, extensive waterways and canals, then automobiles and trucks, and aircraft transport. In the 19th and 20th centuries elevators and escalators move cities ever upward with skyscrapers that became ever more vertical and dense. Kenzo Tange, a Japanese architect, has even conceived of the ArCube that would achieve incredible human habitation density within a cubic structure a kilometer in all three dimensions. This ultra-high density could lead to many potential negative social, political, infrastructure, and especially security and resilience concerns in an age of growing concern with regard to terrorism. The question of what is smart and most viable has clearly changed over

[9] Brian M. Rosenthal et al., "The Making of Meltdown: How Politics and Bad Decisions Plunged New York's Subways into Misery" *The New York Times*, pp. 1 and 26, Nov. 19, 2017.

[10] Daniel C. Vock,"Fixing WMATA, the Nation's Second Busiest Transit System," Governing.com November 2016 http://www.governing.com/topics/transportation-infrastructure/gov-wmata-transit-problems.html.

[11] "The Relationship Between Transportation and Economic Development" Wisegeek.com http://www.wisegeek.com/what-is-the-relationship-between-transportation-and-economic-development.htm#didyouknowout (Last accessed December 15, 2017).

time. The advent of telegraph communications, the telephone, fax machine, radio and television broadcasting, broadband services, the Internet and IT networking, has increasingly emerged as the smart alternative to physical transportation.

In the 21st century it is often proved to be better to move ideas, concepts, visualizations, simulations and services electronically rather than to move people. It is today easier to create distributed telecities and metacities around a core city rather than verticalizing physical structure to create massive density of people. In the book *Safe Cities* the key idea expressed was as follows: "Urban sprawl is bad. Urban density is good, but 'super Urban density' turns increasingly negative again. The solution—at least in part—must be metacities that employ the best new principles of urban planning, the best new technology, and best invoke the spirit of urban pride. It is such new cities that can off load the pressure of super density from the swelling ranks of overcrowded mega cities….As documented by the World Bank, fully 80% of new urban development in a growing number of megacities is represented by slums."[12]

Telecommunications, IT Networks and AI Control Systems

For centuries transportation systems of streets, railroad tracks, highways, and airport hubs have dominated the patterns of urban growth and development. In the 21st century broadband communications are now beginning to serve a new role and are helping to redefine the patterns of growth and the nature of work and commuting within modern countries and cities. If one analyzes patterns of urban development and optimization of levels of density in terms of traffic, crime, resilience to fire, water and sewage systems, natural disasters, terrorist attacks and more there is considerable objective evidence that the use of broadband communications to link urban buildings that max out at 12–15 stories makes much more sense than super densities of mega-skyscrapers that can tower even more than a hundred stories. The experience that is now available from clean air initiatives and telecommuting to work as seen in Tokyo and other Japanese cities, in southern California, and elsewhere around the world indicates the advantage of linking workers via broadband systems. There is now evidence that urban density reaches a point of maximum efficiency and then moves toward diminishing returns somewhere in the 12–15 story levels of density. Much greater density of human interactions and cooperative relationships can of course be created via broadband networks.

There is an ultimate wisdom that comes from the realization that it is easier to move electrons than people. This basic tenet that opts to rely more on broadband networks is environmentally sound, more economically and ergonomically efficient, and much safer in today's complex world. How do you fight a fire in a building over a hundred stories high? How do you efficiently evacuate such a building from a

[12] Indu Singh and Joseph N. Pelton, *Safe Cities: Living Free in a Dangerous World* (2013) Emerald Planet, Washington, D. C., p. 4.

terrorist attack? How do you defend such a building's HVAC or electrical system against an assault or repair it efficiently after such an edifice is fully occupied?

Cities around the world have grown out of control for too long. Urban communities and especially megacities have developed much too fast. This random and nonstructured growth pattern for cities can no longer be the model for the expansion of cities—particularly giant urban regions with populations larger than countries.

Today's cities have too often become inefficient, polluted, congested, and increasingly unsafe. Integrated planning is needed to achieve reasonable efficiency, and transportation, communications and energy systems are key to achieving a reasonable path forward that is sustainable. The common theme that one can see in cities that have been designated "intelligent communities" are that they have applied broadband networks, planning, and network controls to help solve many of their problems. This will be ever more important to 21st century cities as we move toward 80% urbanization of all people on Earth.

The key question that now applies is, how does effective control of cities come about and how is it applied without becoming onerous or even dystopian? The latest capabilities associated with smart data, causal models, and heuristic algorithms can be applied to provide real-time information to urban control. Thus sensors, data inputs and analytics can be used to help traffic jams become disentangled, to provide first responders with real-time information about fire or explosion characteristics, to reveal criminal behavior, and to otherwise provide urban problem-solving capabilities in near real-time.

The commercial business community is already beginning to use smart data and analytics to govern their business practices. The "Doves" of the Planet remote system can monitor the parking lots around the world with less than an hourly update to tell competitors who is shopping where. The Alibaba electronic shopping networking is monitoring customer transactions and "rating" customers and profiling their consuming habits. It is not a long distance from such commercial practices when transferred to urban planning analysis and criminal investigation to profiling citizens as to their "likelihood" of committing crimes.

The short story by Philip K. Dick called "Minority Report" that was transformed into a film of the same name ended up profiling people and identifying them as "murderers" before they acted. This type of science fiction scenario of profiling, rating, and characterizing people is of growing concern to those who fear technological overreach that could threaten freedom, individual choice and the liberty so basic to democratic society.

The availability of pervasive sensors, prodigious processing capacity to analyze the behavior of the citizenry of an entire community is actually of concern if this type of capability is over used. The extreme analysis of smart data based on extreme monitoring of citizen behavior that evokes images that date back to *Brave New World*, and other dark views of the future such *Player Piano,* stand as warnings to limit excessive use of monitoring and "overkill" analysis.

This suggests that laws and regulatory processes must limit just how much monitoring is legal and to restrict smart data to clearly limited applications such as overt threats to public safety and assaults on the integrity of national political elections and the national defense.

Use of "Intelligent" Tools for the Community vs. Abuse Against Individuals

Guidelines and protections against abuses in the use of sensors, monitors, judicial warrants for eavesdropping, and restrictions on governmental profiling of individual's habits, political proclivities, etc., are clearly needed. The use of heuristic algorithms and causal models to project the behavior of urban communities in terms of traffic, patterns of crime, economic growth or recession, or other macro-levels of behavior can be important aspects of effective urban planning. The abuse of these tools to thwart individual political liberty is a significant concern. This presents a key difficulty. On one hand there are the opportunities presented by using these sophisticated smart data tools to support the community needs at a macro-level, versus the abuses that can come by applying these tools to vulnerable individuals. This is a very delicate balance that holds one of the keys to democratic freedom in the future. These concerns will be addressed in greater depth in Chapter 5.

Energy, Power and Environmental Systems

Closely coupled to transportation and broadband communications systems for cities are the energy, power and environmental systems. This three-way blend of vital urban infrastructure is increasingly found in most cities within the developed economies of the world. The same will likely be true in the longer run for cities in the developing world as well. Unless a city has a well-designed and functioning transportation, communications and energy system the rest of the key services such as education, health and medical care systems, water and sewage systems, and indeed all types of business operations will have great difficulty sustaining themselves effectively. One has only to look at locations such as Puerto Rico or the American Virgin Islands, or other areas devastated by Hurricane Irma and Maria, to see how the loss of transportation systems, telecommunications and power systems served to shut down schools and hospitals, food distribution, business commerce, water and sewage systems, and essentially every aspect of normal life both in urban and rural areas. (See Fig. 3.3.)

Other Vital Public Infrastructure

The process of small city planning actually involves reviewing the entire urban infrastructure to seek improvement. Thus the objective of smart city planning and design is to consider the best way to proceed with maintenance, levels of modernization, improved operation, and ongoing upgrades over time. Change and possible ranges of improvement will be constantly reviewed. Improvements could

Fig. 3.3 Devastation, debris and downed utilities from Hurricanes Maria and Irma in Puerto Rico. (Graphic courtesy of U.S. Office of Emergency Management)

be new technology, new software, retraining of workforce, conversion of public labor to private contractors or improved processes. Improvements in utilities such as water treatment, sewage or trash removal on one hand might cut expenses, allow or restrict new development, reduce pollution or labor costs, or improve traffic flows. It is through smart data analysis that these interrelationships and improvements or cost reductions can be discovered.

Public Security, First Responders, and Cybersecurity

Finally public security, first responders, and especially cybersecurity against hackers and techno-terrorist attacks is increasingly important, as smart technology and smart software is employed in modern cities. Security is an increasingly difficult aspect of the smart city. This is because the range of security-related activities keep expanding.

At the extreme end of the scale there are true disaster scenarios from natural events such as earthquakes, hurricanes, floods and tsunamis or an orchestrated attack that disables vital infrastructure. It is ever more vital to take care and have levels of protection to guard essential and potentially vulnerable infrastructure. The

most worrisome concerns are thus not maintenance but inadequate care with regard to possible catastrophic failures. Yet care must be taken to protect key infrastructure and its control software at multiple levels.

One such possible example of infrastructure failure could be triggered by a possible massive electromagnetic pulse (EMP) event. This type of EMP could also be triggered by a nuclear explosion in space, but much more likely would be a massive solar storm such as the Carrington event of 1859, or a recently discovered earlier event chronicled in Chinese records from the 18th century.

A large enough coronal mass ejection (CME) from the Sun that fries electrical transformers around the world is a growing concern as modern megacities expand across the globe. A giant solar storm that could disable electronic grids around the world and leave nuclear power stations subject to ultimate meltdown if electrically powered pumps cannot be restored in time is a true modern concern. With over 700 nuclear generators around the world that produce electrical power and carry out research, the possibility of a global disaster could emerge in the event of a major solar storm that triggers a worldwide EMP. All nuclear power plants, of course, have diesel-powered water pumps that cool the nuclear power plants and prevent their meltdown, but diesel fuel supplies are not sufficient to withstand outages that might last months or longer.[13]

Conclusions

Modern advanced and intelligent infrastructure is the foundation for building smart cities. Smart infrastructure can provide improvements to a city's efficient operation, provide for reduced staffing and costs, and in some instance provide key improvements in a number of areas. An expanded broadband network can, for instance, aid education, healthcare, transportation, energy network controls, security and first responder effectiveness, and even water, sewage and trash operations. This would be the case only if there is interagency cooperation and a willingness to leverage gains across shared infrastructure and software.

Smart infrastructure alone does not make a smart city, but it sure can help if done right. The smartest thing of all is deciding which upgrades will make the most positive impacts and when to and how you decide to make these changes. Installing the latest gadget or gizmo is not the objective. It is deciding, based on good data and analytics, which changes and upgrades will produce the most bang for the buck. Also needed is the active involvement of the citizenry in such upgrades in order that they understand what improvements will result and how they will benefit; this is an essential part of the process.

[13] Ken Jorgustin, "After the EMP comes Nuclear Meltdown" Modern Survival Blog, February 22, 2014. http://modernsurvivalblog.com/emp-electro-magnetic-pulse/after-the-emp-comes-nuclear-meltdown/.

Chapter 4
Cyber Defense in the Age of the Smart City

The number one problem in trying to create effective cyber defense systems for the next decade will most likely come from looking through a rearview mirror to anticipate problems. Cambridge Analytics, which "appropriated" the personality profiles of 50 million users of Facebook and then bombarded them with a view of "news" distorted to conform with their political views, is just one example of a cybersecurity problem that has emerged from the research on the latest U. S. presidential election. Each new edition of industrial controls, machine-generated commands to control automated infrastructure and artificially intelligent algorithm will reveal a new type of cyber weakness that urban planners must contend with and hopefully solve.

The future of information technology and data systems is undergoing a fundamental transition. Cybersecurity is thus going to be radically different a year from now, 2 years from now. Another decade will entirely change the landscape of the meaning, import and academic content of what we call cybersecurity today. If smart cities are to introduce positive change in the lives of citizens and business people that live there we must have positive change on the cybersecurity front. And this will have to be big change, with the re-engineering of most computer systems that cities now depend on for daily operations. The cyber-attack on the city of Atlanta in 2018 was by a ransomware gang named SamSam that was seeking $51,000 in ransom payments via bitcoin transfer. This attack brought many of Atlanta city functions to its knees, and city after city will follow until reform is completed.

Atlantic Monthly writer Ian Bogost, who was personally affected by this ransomware attack, has summed up where we are today in terms of urban cyber vulnerabilities: "Decades of wonky, half-baked, Internet-connected systems, popularized and exposed to invite risk, have lowered expectations so much that nobody is even surprised when they don't work for days at a time. As more urban infrastructure, including smart-city systems, go online, cities and their citizens should be terrified by the Atlanta ransomware hack. But for now, it isn't even really considered an infrastructural

© Springer International Publishing AG, part of Springer Nature 2019

J. N. Pelton, I. B. Singh, *Smart Cities of Today and Tomorrow*,
https://doi.org/10.1007/978-3-319-95822-4_4

catastrophe. It's just a 'massive inconvenience,' part and parcel of living with those bonkers things called computers. After all, what else are you going to do?"[1]

The required changes will truly be demanding for those cities that take the challenge seriously. The transformation in cyber systems and nature of software and online content will be more basic than most systems' engineers now anticipate. Some cities, such as Dubai and Singapore, that are moving to block-change ledger systems to protect their vital data and infrastructure are on the right track. Such protective digital security systems are essential to the future. This is because the change coming to smart cities will be in the sheer volume of data networking, the surge in data generated from automated and artificially intelligent sources and the all-encompassing Internet of Everything. Just one of the artifacts of this change will be the almost violent increase in available 'access points' vulnerable for ever-increasing cyber-criminal activity. And why is this increasing? *The New York Times* reported that the cyber-gang that engaged in "one of the most sustained and consequential cyber-attacks ever mounted against a major American city," when it attacked Atlanta, Georgia, has now made over $1 million this year in its ransomware attacks on cities. Local, national and international law enforcement clearly has to be increased against cyber-criminals, but significant new cybersecurity is needed as well.[2]

In short, we are not ready for such a data-rich future and an increasingly autonomously networked world. Studies by Intel and its data security analysis subsidy known as Wind River have made a number of key projections for the future. Others have made somewhat similar forecasts, but the Wind River assessments are among the most startling—and very possibly true.

Their projections suggest a "super automated" world that has surging levels of direct machine-to-human and machine-to-machine interactions and data that is machine generated and perhaps dominated by automated systems. In this new data-networked world, automated data systems will increasingly predominate with a very rapid ramp up in data and a huge number of data sources. As noted in the Introduction to the Wind River report, the Internet of Things Defense White Paper and other similar studies suggest that within the next 5 years there will be a remarkable change due to the rapid addition of IoT-enabled devices.[3]

This was already discussed in Chapter 1, but for emphasis we will repeat some of the quite remarkable—yet creditable—forecasts. In the next 4 years there could perhaps be a 50-fold increase in stored data. In addition to this Niagara-like increase in stored data, everything else will change as well. Today 80% of data is unstructured, but in 5 years it will largely be structured. Also today 85% of all devices are not connected via the Internet or have other networking capabilities. Yet in 5 years the great majority of all devices will be connected via the Internet of Things,

[1] Ian Bogost "One of the Biggest and Most Boring Cyberattacks Against an American City Yet" *The Atlantic* Mar 28, 2018 https://www.theatlantic.com/technology/archive/2018/03/atlantas-boring-ransomware-attack/556673/.

[2] Ibid.

[3] "IoT in Defense White Paper," Wind River, http://www.windriver.com/whitepapers/iot-for-defense/wind-river_%20IoT-in-Defense_white-paper.pdf. (Last accessed June 6, 2016.)

Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) networks, or cloud-related connectivity. This Wind River study also projects a 15-fold increase in machine generated data from the end of 2016–2020.[4]

Although this surge in data growth and machine-generated data may start to slow as of 2020, the amount of data that is machine-generated and the amount of stored data that might be available on networked systems could still grow to be truly staggering—more than a hundred times today's levels and within just another decade.

To say that we are unprepared for this digital future in terms of storage capacity, systems security, or protection of vital infrastructure is to understate the problem greatly. The risks are everywhere. These include theft of networked data, cyber-terrorist attacks on vital infrastructure, illegal access to billing records, or loss of public funds. Even the ability of civic professionals to cope with the sheer volume of digital information in the age of the Internet of Things is a challenge. Urban computer experts will be faced with databases that will soar into the petabyte or zettabyte range or even higher. How this information will be securely stored and accurately processed represents a whole new series of issues. These include vital questions such as the best methods to use in accessing the cloud and how to do so effectively and securely. How does one maintain digital security when millions of IoT access points can send and receive data? And these are just the start of questions concerning digital security.[5] Some believe the advent of block chain technology can provide a new level of security to digital networks. Others believe this highly secure way to store and retrieve data will prove to be a highly dangerous digital playpen where cyber-criminals, hucksters, and even techno-terrorists will go to play.

If one mixes into this a host of new appealing "apps" that consumers find appealing but digital criminals and political spin artists find to be fertile territories to exploit the dangers to an unsuspecting citizenry, these efforts will only increase. One of the scariest things we have recently heard said is the following cogent insight: "If there is an appealing new 'free app' out there made available for you to exploit, just remember you, your eyeballs, your personal profile, and your behavioral profile have just become the product." In this new world, personal privacy, protection of your digital and financial assets, and cybersecurity are hard to separate and wall off from one another.

Sensing devices in space, such as hyper-spectral remote sensing satellites, are just one example of an overly rich digital networked world. These satellite systems can produce ginormous bytes of digital diarrhea. Data centers can be massively overloaded in only a short span of time if care is not taken. Too high levels of resolution of data over small bandwidth of spectrum can overwhelm analysts and produce so much data that it cannot possibly be efficiently processed and used. This is just one instance of machines that can churn out too much information. It is not only a matter

[4] The Internet of Things for Defense: A White Paper, Wind – An Intel Company, October 2015. http://www.windriver.com/whitepapers/iot-for-defense/wind-river_%20IoT-in-Defense_white-paper.pdf.

[5] Ibid.

of security of data. It is a matter of populating the world with too much "passive information," i.e., what Professor Tanaka of Japan has defined as more incoming information than people can reasonably use—let alone adequately protect.

The Importance of Network Security

The world of digital networking that cybersecurity professionals are trying to understand and defend is large and complex. This is true for several reasons. The most obvious reason is that digital networking now embraces virtually every aspect of life on Planet Earth. The applications and digital technology required to support all of these millions, if not billions, of applications are understandably quite diverse. The programs that might be supported in just a single school district to support educational applications may be in the several hundred.

The second reason is not as immediately obvious. This is the historical reason. Digital networking, as it is employed today, grew up in different user communities with different purposes in mind. Some networking-oriented organizations were focused on creating technical standards to allow data exchange and interfaces to be established, while telecommunications organizations were addressing the needs for voice, radio and television distribution.

First in this process were the telecommunications engineers. They were initially focused on communications and moving information from point A to point B. Next up in the development process came the world of broadcasting. In this case the engineers were focused on distributing audio and video information from a single point to a large and broadly distributed audience. Finally came the computer applications community. This community was involved with processing data and moving it through digital networks that first sought to connect mainframes, but this was only the start.

Now digital network engineers seek to link all sorts of computers, communications and entertainment devices and in a great variety of ways, and this is chopped up into packets that can flow through digital networks with "headers" that tell how the packets can be reassembled in the correct way. The various types of networking usage now range quite widely from short tweets to full length movies. There is today a need to connect the vast processing power represented by supercomputers to network servers and routers, personal computers and smart phones. The geographic range also goes from quite small to global in scope. Digitally distributed networks may be connected in small local area networks all the way up to global enterprise networks with millions of linked personal computers. These wide area networks (WANS) can support a worldwide airline booking network, a global retailer or banking system or a governmental operation on what are called "intranets."

There is far more traffic on closed and protected intranets than on the Internet. The latest computer networking era represents yet another explosive growth requirement. New digital networking needs now involve the Internet of things (IOT) and Supervisory Control and Data Acquisition (SCADA) networks, where the number of interconnected devices reaches up into the billions. In this new world of computer applications the networking involves automatic device

interactions, machine-to-machine communications and processing of data generated autonomously by literally billions of sensors, meters, counters, gauges, and collectors of various types of information with nary a human in sight.

There are now scores of organizations, such as the International Telecommunication Union (ITU), the Internet Engineering Task Force (IETF), the European Broadcasting Union (EBU), the International Standards Organization (ISO), the Institute of Electrical and Electronics Engineers (IEEE), the Motion Pictures Experts Group (MPEG), the European Telecommunications Standards Institute (ETSI) and on and on involved in developing standards to allow computer networking and interface standards. This gives rise to complexity, a torrent of change in standards, and, not surprisingly, vulnerability to cyber-attacks.

Unfortunately digital networks can be attacked at a great number of different levels. There can be attacks and interception via various transmission modes and at telecommunications switches and computer routers, via those who have developed the means to decrypt encrypted messages. At the most basic level these attacks involve one of two things. The attack can involve obtaining and using for unauthorized purposes private information, or it can involve installing or otherwise manipulating various types of "malware" that does harm to data or networking systems capability. Sometimes this is done simultaneously by capturing information then deleting it or sabotaging it at the same time. These activities can range from modestly harmful attacks—falsely assumed to be mere pranks—to horrendous events such as major criminal attacks on institutions, cyber-terrorist assaults on vital infrastructure, or even true acts of war. Often cyber-attacks are sorted into three categories of attacks: on individuals (Category One); attacks on institutions such as banks or airlines (Category Two); or attacks on nations (Category Three).

Basic Background

The first step in understanding this is to define key terms and cyber defense concerns into a number of well -defined areas so that the scope of data use and protection problems can be well understood. This structure can then allow various strategies to be developed in order to cope with cybersecurity, and defense. These can then be divided into reasonable areas for analysis, risk assessment, and strategies to be used against network intrusions. Such efforts can increase security to the maximum degree possible.

The approach taken in this book is to understand the basic importance that digital networks play in our lives today. There is now a fundamental interconnection that links the cyber-based" Digital World" and "Physical World." This vital linkage in terms of security, business operations, etc., makes these two worlds almost inseparable. An attack starts in cyberspace has real, concrete and in some cases devastating impact on the real physical world. It is more and more the case that the "brains" and thus the actions of the physical world have been transferred to the digital world and thus digital processors control most of the modern world most vital and basic infrastructure. The exponential growth of the Internet of Things (IoT) linked devices and

Supervisor Control and Data Acquisition (SCADA) controlled infrastructure that are key features found in smart city architecture raises the ante for those seeking to provide resilient cyber security capabilities in the modern world.

It makes no sense to say something like we need to protect our vital infrastructure, our business, economic and financial institutions and, oh yes, our digital networks as well. This is because these systems are today essentially one and the same. Our power systems, our transportation networks, our water and sewer systems, our manufacturing industries, our banking and insurance systems, our police and national defense forces, and indeed everything in modern society is connected to and controlled by our computer and communications networks. One step forward that has now been taken in this regard is via the Department of Homeland Security (DHS) in the United States. This U. S. agency has now introduced the Einstein system to protect the U. S. federal government across all agencies via a software system known as "Einstein". Einstein first seeks to detect and block cyber-attacks from penetrating and compromising federal agencies. Second, Einstein provides DHS with the situational awareness and other AI techniques to use threat information once detected in a U. S. agency to aid in protecting the rest of the U. S. government. It is now expanded so that it can also help the private sector and other governments also to protect themselves. Einstein 3, which was introduced in 2013, is adept at blocking malware and works in tandem with Internet service providers. The threat indicators that are used by Einstein 3 are generally based on traffic metadata. Indicators of malware threats can include IP addresses and packet payload. The design of Einstein 3 has been aimed at defining indicators that are specific enough to help in identifying malware threats while general enough to protect the privacy of legitimate traffic.[6] The ability to identify such automated cybersecurity protocols and AI algorithms is key to the future in light of the exponential rise in traffic that is now projected.

If one takes just one element of the smart city, such as transportation systems, one finds that digital networking and control systems are enmeshed everywhere in their operation today. SCADA networks change the timing of traffic signals to accommodate the needs of rush hour flows. IoT-linked devices are now everywhere in smart transportation systems. They are embedded in taxis, buses, metro cars, trains, planes, and even elevators and escalators, providing for effective lighting, signaling the breakdown of key components, and assisting with security monitors. (See Fig. 4.1.)

In short, it is essential to realize how integrated the digital world and the physical world are in today's communities. Everything is connected to and controlled by digital networks. This includes cars (i.e., those equipped with smart fuel injectors and IoT components), trains; aircraft; traffic lights; electrical power grids; water and sewage pumping stations; banking systems; hydroelectric dams; transformers; pipeline operations; security surveillance systems; banking transaction networks; stock markets; industrial production machinery; and so on.

Sure people in many of these operations are involved. Usually people can shut systems down and/or start them up again. This is why the human-machine interface

[6] William Jackson, "Einstein 3 goes live with automated malware blocking" GNC, July 24, 2013 blocking https://gcn.com/articles/2013/07/24/einstein-3-automated-malware-blocking.aspx.

Fig. 4.1 The flow of rush hour commuters and airport passenger is aided by SCADA and IOT-linked devices (Illustration courtesy of Washington Metropolitan Airport Authority.)

(HMI) stations in so-called SCADA industrial control systems are so important. But most day-to-day and minute-to-minute human controls are systematically being phased out while computer processing and smart heuristic controls are being phased in. Automated industrial controls are making more and more decisions concerning the functioning of infrastructure and other elements of modern communities. Whether we like it or not machines are increasingly in control of much of modern life albeit below the surface so that it is not readily apparent.

But today cars are moving toward becoming driverless and aircraft are often on autopilot even for landings. The controls can be specialized software or control systems for robotic devices, and there are now many types of these systems. The following, however, are the most important systems for automated control and IT systems networking today. These are briefly defined below.

Potentially Vulnerable Digital Systems

These are digital networks that allow control commands and relay of remote messaging of problems and key data points. These SCADA systems are typically designed for networks such as large-scale pipelines, electrical grid operations, traffic signals, water and sewage systems, and other such types of infrastructure.

The automating of these systems can allow for the systems to operate more efficiently and greatly reduce labor costs and with much greater accuracy, reliability and flexibility such as to time shifted activities to adjust to peak and valley operations over daily or weekly cycles. These systems not only provide control but also collect data from remote locations as to operating conditions in essentially real time.

The most pervasive type of industrial control systems (ICS) today are actually SCADA systems. There are, however, simpler and less elaborate systems that are known by such names as distributed control systems (DCS), or other even smaller and simpler control system configurations such as programmable logic controllers (PLC). In the case of PLCs, they do not usually collect and transmit remote data, but simply control machine production or maintain automated operations.

Internet of Things (IoT)

The most significant new element with the largest exponential growth is the design of Internet connectivity into a wide range of products such as automotive vehicles, ships and aircraft, various utilities such as refrigerators, washing machines, ovens, and indeed almost any type of machinery that has components that wear out, cycles of operation and warranties. Manufacturers, via the Internet and Wi-Fi networking or other forms of Internet/intranet connectivity, can monitor the performance of their products and improve reliability and effectiveness of performance.

This type of capability was first designed for monitoring defense-related performance and operational efficiency, but it has now become a worldwide phenomenon. The technology has almost unlimited potential to increase performance and efficiency of operation, but the misuse of the technology allows for cybersecurity abuses. We have reached the age of smart refrigerators being able to be the source of global spamming. Ironically, the technology that was developed by the U. S. Defense Advanced Research Agency, DARPA, may become the greatest threat to smart U. S. defense systems.

RFID Tracking and Inventory Control Systems

This is another key communications capability that is being used to track billions of items in modern retailing and industrial inventory control. This radio frequency ID technology allows companies to handle many millions of items a month on a fully automated basis.

Cloud-Based Networking Access

The storage of massive amounts of data in the cloud from many sources plus the ability to process data on cloud-based systems creates a wide range of potential vulnerabilities via the networking access channels.

Digital Communications Networks

There are today a myriad of digital communications networks to businesses, governmental agencies and individuals, and none of these are guaranteed to be secure against hackers or malware attacks. These communications networks include public switched telecommunications networks (PSTN), private IP networks such as enterprise networks, Wide Area Networks (WANs), Metropolitan Area Networks (MANs), Local Area Networks (LANs), virtual private networks, plus Wi-Fi and Wi-max systems. The terms are defined in greater detail in the glossary.

The speed of access provided by broadband systems continues to increase. This will surge with the projected increase in stored data and the hyper-growth of digital interactions. Again this will increase digital vulnerabilities. In the age of RFID and the Internet of Things billions and then trillions of smart devices will interact over an unimaginably large number of electronic and photon-based links. Cyber density thus will become exponentially larger throughout modern society. Thus cybersecurity will become more difficult to develop and implement on a timely basis.

These various types of digital networks involve transmission media of various types, switching nodes and digital routers and software that perform a variety of functions. In the modern world of data exchange the two most important data exchange systems are the Open Systems Interconnection (OSI) model that are used to support the public switched telecommunications network (PSTN) and the system used within the Internet system, which is the Transmission Control Protocol/Internet Protocol (TCP/IP). The importance of these two reference models and the need for improved methods of cyber-defense that relate to both are discussed at length in Chapter 6 with regard to the analysis of issues related to the Internet of Things.

These OSI/PSTN and TCP/IP data exchange systems unfortunately are both subject to cyber-attack. There is vulnerability to attack during the transmission over various media or at the telecommunications switches within the PSTN, at points of presence (POPs) and within Internet/intranet systems at the routers and now even at Internet of Things enabled devices.

Figure 4.2 provides a breakdown of the various layers within the OSI model and provides examples of usage for telecommunications and data networking. In Chapter 6 the relationship between the seven-layer Open System Interface (OSI) reference model and the simpler four-layer TCP/IP reference model are discussed along with the difficulties that connecting these protocols together can bring.

Overview of Digital Transmission Media

A key aspect of cyber security relates to the various types of transmission media used to transmit information. Essentially this divides into wire and wireless transmission systems that will be briefly discussed and defined below.

OPEN SYSTEMS INTERECONNCTION (OSI) MODEL with EXAMPLES of USAGE				
Layer		**Protocol Data Unit (PDU)**	**Function**	**Examples**
Host layers	**Level 7 Applications**	**DATA**	High-level Application Protocol Interface including resource sharing, remote file access, directory services and access to virtual terminals.	NFS, SMB, MFS, SFP and FTAM protocols.
	Level 6 Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption.	CSS, GIF, HTML, XML.
	Level 5 Session		Managing communication sessions, i.e., continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes	RPC, SCP, PAP, FTP, HTTP,HTTPS, SMTP,SSH, Telnet,
	Level 4 Transport	**Segment (TCP) / Datagram (UDP)**	Reliable transmission of data segments between points on a network, including, segmentation, acknowledgement and multiplexing.	TCP, UDP
Media layers	**Level 3 Network**	**PACKET**	Structuring and managing a multi-node network, including addressing, routing and traffic control.	Apple Talk, IPsec, IP versions 4, 6 or 7
	Level 2 Data Links	**FRAME**	Reliable transmission of data frames between two nodes connected by a physical layer	IEEE 802.2, LLDP, PPP, MAC, ATM MPLS
	Level 1 Physical	**BIT**	Transmission and reception of raw bit streams over a physical medium	DOCSIS, DSL, Ethernet, Physical layer ISDN, and RS-232

Fig. 4.2 OSI model systems

Fiber Optic Networks

These high efficiency transmission media are becoming more and more predominant for high speed broadband transmissions over long distance urban-to-urban or trans-oceanic connections. The coherent light laser transmissions through fiber optics are able to deliver enormous throughput capabilities with multiple strand fiber networks able to transmit at rates even up in the terabits/second range. These fibers also deliver near zero bit error rate transmission quality and are quite secure in that it is hard to intercept messages that travel on such networks. Currently these systems use the lower cost red lasers. Eventually green and blue lasers in even higher frequencies will be able to operate at even higher throughput rates. Today cable television networks with fiber networks in the ground make 'dark fiber' cables available to other businesses and even governments to support a variety of commercial or municipal services.

LED Fiber Systems

These lower speed fiber optic systems utilize light-emitting diodes (LEDs) and employ incoherent light and are much less costly. These are also relatively secure against interception but support slower throughput services.

Coaxial Transmissions and Ethernet

Many cable television and local area networks operate using coaxial cable to transmit information. These are lower in cost to install and operate but also perform at lower speeds. These types of systems are used in many business, commercial and industrial applications to provide metropolitan area networks (MANs) that connect a number of business site locations within a city.

Broadband Wireless Transmission (Microwave Relay and Millimeter Waveguides)

The alternative to wire, coaxial cable or fiber transmission for data relay over distances has been microwave relay. Due to the curvature of Earth and broadcasting strength, microwave relay towers have to be built at regular intervals, typically some 15–30 miles (or 24–48 km) apart. Microwave towers on top of mountains and in favorable climes can be even further apart. The advent of fiber technology has tended to render microwave relay for long distance telecommunications obsolete, and

frequencies allocated for this purpose have tended to be reassigned to other applications. The higher throughput capability of millimeter waveguides has seen the use of this technology for line of sight broadband mobile applications in urban areas in countries such as Japan.

Infrared Communications

Even high throughput wireless systems for limited distances have been utilized for applications such as intra-office communications or links between buildings. These are also line of sight systems and can have interference with other uses such as communications to toys with remote control signaling that use infrared links.

Wi-Fi and Wi-Max Hotspots

The largest upsurge in urban communications has been to create Wi-Fi hotspots in such locations as hotels, cafes, public libraries and even broader reach Wi-max coverage areas. This is also used for wireless routers in local area networks for offices. The Institution of Electric and Electronic Engineers (IEEE) has developed the IEEE 802.11 standards for this wireless service. These standards cover various media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands. The IEEE 802.11N wireless LAN with two antennas can support speeds up to 300 megabits/second and a range of several hundred feet (using the unlicensed 2.4 GHz frequencies. There is a new 802.11AC standard that can cover an even wider range and speeds up to 1 GHz and thus quite broadband applications (Wireless B, G or AC).[7]

Wi-max refers to interoperable implementations of the IEEE 802.16 family of wireless-network standards ratified by the WiMAX forum. (Similarly, Wi-Fi refers to interoperable implementations of the IEEE 802.11 Wireless LAN standards certified by the Wi-Fi Alliance.) While IEEE 802.11 covers the standards for wireless Local Area Networks, IEEE 802.16 covers the standards for metropolitan area networks (MANs). Wi-max wireless networks are intended to cover a larger area and support broadband throughput rates for many urban users. Both Wi-Fi and Wi-max wireless systems do not provide security to users, and thus one should not carry out financial or confidential matters via such system**s.**

[7] "Wireless B vs G vs N vs AC | What Is the Difference?" http://homenetworkadmin.com/wireless-b-vs-g-vs-n-vs-ac-difference/ (Last accessed Nov. 14, 2017).

Satellite Interconnections

Satellites are used for a wide range of communications for television and radio programming, connectivity to remote locations where fiber and coax are not available (i.e., deserts, jungles, mountainous areas, swamps, etc.), digital networking for credit card validation, remote banking, multi-casting, and global enterprise networks. Close to half the nations of the world connect to the Internet via broadband satellites. Digital Video Broadcast with return channel services (DVB-RCS) is used extensively for broadband data services where service to the "edge" is needed and connectivity is in flux. This particularly applies to military satellite communications on both dedicated defense satellite networks and dual use of commercial satellite networks for military applications. Today most satellite interconnections are digital and employ either time division multiple access (TDMA) or code division multiple access (CDMA) that is popularly known as spread spectrum. Many of the satellite systems today operate from geosynchronous (or Clarke) orbit, but currently there are plans to deploy more and more constellations of satellites in medium Earth orbit or low Earth orbit to provide Internet optimized services that because of their low altitudes have minimal delay or latency. This lack of latency makes LEO constellations particularly well suited for digital networking applications.

High Altitude Platform Systems (HAPS) and Unmanned Aerial Systems

Yet another mode of wireless communications that is just starting to emerge is now known as high altitude platform systems (HAPS) and unmanned aerial systems (UAS). Such systems involve lighter than air craft, autonomously piloted aircraft, and even craft that are powered by solar cells or beamed energy that could be deployed to provide various types of telecommunications services. Frequencies have now been allocated within the International Telecommunication Union (ITU) for such applications that may prove useful for island countries or for defense-related purposes. Again the lower altitude of these systems make them well suited to digital networking purposes because networked systems are not optimized for the long transmission delays associated with geosynchronous satellites in Clarke orbits that circle Earth in orbits with altitudes of 35,870 km. These orbits out almost a tenth of the way to the Moon are fine for broadcasting and even communications with their one-quarter of a second transmission delay, but commuter networks work better with virtually no latency or transmission delay of any perceptible length.

Network Security for Different Transmission Systems

Wireless systems are designed for a large number of users to access a network and do so with flexibility. This flexible access does come at some cost in that these mobile transceivers are less secure against interception and cyber-attack. Further in a large wireless network, a hidden and unauthorized node is easy to conceal. This strongly suggests that any such wireless network should rely on strong encryption for protected communications. The assumption that a hard-wired network is thus a secure transmission system does not necessarily follow. There are ways to insert transmission interceptors at switches, network terminals, even within a "wire" system to intercept systems. Sophisticated limpet technology can even be devised to intercept signals being transmitted on wire systems. The bottom line is that security needs to protected at all levels—in transmission systems, at transmitting or receiving terminals, within telecommunications switching centers and routers, and by quality encryption and de-encryption systems. Even if precautions are taken at all levels, there is still the danger of systems operators, who have access to codes. Those who know the passcodes or who decrypt messages can always inadvertently or intentionally defeat the best of cybersecurity systems in a digital network.

The Smart City and Cybersecurity Challenges

This book describes cybersecurity challenges in the following terms: interconnectivity, complexity, and the increasing scale, diversity and automation. These all will represent increasing concerns with regard to security within data networking and telecommunication networks. The largest challenges that will be addressed and analyzed will be those involving the following: (1) increasing volume of digital interactions; (2) the rise in mobile applications and communications; and (3) the increased level of use of artificial intelligence in digital networks and machine-to-machine communications. All these challenges result in the need for more sophisticated strategies.

There are all sorts of potential ways that an urban services network can be compromised. In late December 2017 U. S. attorneys formally charged two Romanians for having sent out spam messages infected with a ransomware virus to a large list of e-mail users. This ransomware attack ended up disabling nearly 200 surveillance cameras in the Washington, D. C., area. This was part of a broader cyber extortion ring attack that also disabled many other computer users. Initially it was not clear whether the extortion ring was even aware that it was seeking to extort money from the Washington, D. C., police department and that their actions served to disable a substantial number of the city's camera surveillance network. Priority attention was devoted to tracking down these cyber-criminals to determine whether this was simply an effort to extort money in exchange for restoring computer access or whether this was part of a terrorist attack. There was particular concern because these activities all occurred several days before the U. S. presidential inauguration from January 12 to 15, 2017.

In this case all of the infected cameras were taken offline, new software installed and service restored without paying any ransom. In this case the attack was initiated using a British healthcare company IP address that had been hacked, and the health care organization was completely blameless in this attack. Other members of the hacker extortion ring were arrested in Europe and are being tried there. This particular case was insightful in that is showed: (1) weaknesses in the antivirus used in the case of the D. C. police force; (2) the potential overlap between a cyber-criminal activity and a techno-terrorist attack; and (3) the forensic expertise of computer cyber-defense agents and their ability to track down organized cyber-criminals around the world even though it took several months to complete the investigation and arrest.[8]

Effective cyber defense also requires a multidisciplinary research approach. It requires not only in-depth knowledge of IT, software and systems engineering concepts, but also consideration of relevant economics, law and social sciences. Cyber defense must indeed be seen from a system perspective. Comprehensive cybersecurity measures to be effective must take a holistic approach and be seen as a "living" ecosystem. The importance of this broader picture is addressed throughout the book.

Key Components of Protecting the Smart City

This chapter and some of the later chapters in the book are designed to provide up to date information on various information and communications technologies and their relevance to implementing smart city infrastructure. These at the same time also address related urban security concerns and weaknesses in information and communications networks where enhanced protections are needed. Here are some of the most important areas where urban planners need to know more about key new capabilities that can be used to provide smart city services as well as vulnerabilities where more protections against cyber-attack are needed.

1. *Mobile Services.* This is a review of broadband mobile services, new emergency services networks that can be utilized to enhance public safety and a review of mobile apps vulnerabilities and related cybersecurity practices.
2. *The Dark Web.* There are a growing number of problems presented by the dark web that urban planners should be aware of and alerted to. It explores strategies that individuals or businesses might undertake to protect against dark web-based intrusions. This chapter can provide examples of digital defenses against cyber-criminal attacks and explain how assaults can occur at both the wholesale and retail level.
3. *The Internet of Things (IoTs).* This is one of the most important chapters since it addresses one of the most important new areas of cyber-system capabilities. This covers an exploration of where new cybersecurity strategies and opportunities exist as well as where new cyber-defense systems are needed.

[8] Rachel Weiner, "Romanians Charged with Hacking," *Washington Post*, p. B5.

4. *The Cloud.* The effective use of the cloud and super computer capabilities is a source of great productivity gains, but it also, at a variety of levels, exposes users to vulnerabilities and requires enhanced cybersecurity practices and tradeoffs between projected performance and digital defense. Thus there are many aspects of using cloud-based services that city planners need to know.
5. *Security for Industrial Control Systems.* This addresses the numerous digital vulnerabilities that exist with regard to various types of industrial control systems (ICS) and especially the very widely used SCADA systems. The analysis considers not only potential attacks by hackers, industrial crackers, or even techno-terrorists but vulnerabilities by natural events such as fires, industrial accidents or natural catastrophes such as coronal mass ejection events or solar storms.
6. *Space and Cybersecurity.* The extent to which the global economy is now dependent on space systems such as telecommunications satellites, global navigational satellite systems, and even meteorological or surveillance satellites is not widely understood. The need for protective actions to back up satellite applications systems and to provide enhanced security is addressed in this chapter.
7. *EMPs and Coronal Mass Ejections.* The emphasis on most digital defense systems is on attacks by hackers and prevention of intrusion by cybercriminals using malware, as it should be. The extent to which there is a need to consider natural events such as coronal mass ejections and changes to Earth's magnetosphere is a topic of significant concern since these events might not impact a single corporate network or governmental system but actually have devastating global impact. This chapter addresses these potential vulnerabilities on a planetary scale.
8. *Cybersecurity for Military Systems.* This is a topic of major concern and an area where special capabilities and processes are necessary. At one time a few countries were highly dependent on digital networking for their military security, but today an ever-increasing number of countries depend on digital networking for coordinating and operating their defense capabilities. Some of the digital defense practices and capabilities are the same, while others are unique to defense-related networking and controls.
9. *Diagnostic Systems to Discover Cyber Vulnerabilities.* The start to improved digital defense systems is the ability to detect and understand the nature of system intrusions and to know from where the attack on networks originated. This chapter addresses the latest methods to discover and report on cyber vulnerabilities.

Conclusions

The purpose of this chapter was to review the latest information on smart city planning, implementation, and operation in the context of cybersecurity protection. It is important for city planners, administrators, and political figures to all consider what being a smart city means and how to move forward toward achieving the right tools

and processes to make an urban area more intelligent in all aspects of its operation. In carrying out this exercise it is of particular importance to consider the vital role of security and how it can best be achieved within a smart city. This is because smartness can both add key security features but also add new potential elements of vulnerability. It is thus important to consider and detect any emerging vulnerabilities, implement new intrusion detection and protective action, and more—both for the short term and on a longer terms basis. In this chapter and several that follow we have sought to probe the best practices and the note some of the best research efforts to improve digital defense capabilities. These include practices both in the United States and globally.

Thus we have sought to present the latest information and practices to improve digital defense around the globe. Further we have also tried to present areas of research to develop new cybersecurity practices and to develop improved digital systems and software that can better help to provide security against unwanted intrusions, criminal and even techno-terrorist attacks against a city and its automated infrastructure systems. The latest research efforts by the National Security Agency (NSA) to develop new digital defense are not just focused on detection of dangerous malware since this is constantly in flux, and new viruses and ransomware seem to be constantly generated. No, the latest emphasis is on finding ways to authenticate and recognize so-called "white networks" that are confirmed non-hazardous and non-dangerous sites from which to accept messages and to block all other incoming messages and foil attempts to access highly protected sites.

The danger that still remains is that of insider attacks from someone who reveals the needed access codes. Even the most protected sites can become a danger if a trusted user of that site, either by intent or by means of trickery or deceit, might turn a trusted "white site" into a danger zone.

In chapters to follow we provide advice and information about new protective strategies for smart cities that are now being implemented around the world. These areas include key new capabilities that can add tremendous improvements but also include vulnerabilities. These include new developments related to the Internet of Things, expanded use of the cloud and vulnerabilities with regard to mobile communications systems. These discussions and shared research that is provided are intended to provide additional tools and/or useful information that can help urban planners as they plan their city's future. There needs to be vigilance in protecting modern cities against cyber-attack, natural disaster or other problems that might beset an urban center. The old axiom may still be true: "An ounce of prevention is worth pound of cure."

Today, however the ratio may well have changed. Indeed a prevention may be a hundred times if not a thousand times more important than a very expensive cure that could cost much more than we would ever wish to spend. In this regard the biggest danger may not be a cyber-attack but rather a super solar storm bigger than the Carrington event of 1859 or a city-killing space rock bigger than the 40-m Tunguska asteroid that devastated Siberia in June 1908. As more and more people live in giant cities, protective strategies need to be broader and broader in scope.

Chapter 5
Using Intelligent Data Analytics for Urban Planning and Design

The key to any smart city begins with a focused planning process. This effort, if conducted properly, has only a single purpose. This is to define on a collective basis the current situation of a city and where it wants to go in the near, medium and longer term. Personal experience with smart city planning has indicated that cities do not change overnight. It takes hard and dedicated work and continuity of purpose. The Danish city of Copenhagen began planning to become free of dependence on petroleum and energy resilient in the 1970s when a severe oil shortage drove planning in this direction. They now expect to fully reach their goal of a zero-carbon footprint as of 2025, but it has taken some five decades of effort to reach this objective.[1]

Arlington County, Virginia, a special urban area that in many ways complements Washington, D. C., and hosts many U. S. federal agencies, has transformed itself by agreeing to a long-term county improvement plan that centered on development around Metro stops in the late 1970s. This long-term plan, executed over a 40-year period, served to revitalize its retail areas and allowed 85% of all the county's key high-rise development (housing units, hotels, businesses, federal offices, airport and shopping areas) to be concentrated on 15% of the county's land.[2] Today Arlington is embarked on a new 40-year-long plan to transform its energy and atmospheric profile to be cleaner, smarter and more sustainable.[3]

There is great truth to the idea that you will never achieve your goals if you don't know where you are going. It is also true that a community that can dedicate itself to a significant improvement plan and sustain it for a number of decades will succeed

[1] "Copenhagen's ambitious push to be carbon neutral by 2025" http://e360.yale.edu/features/copenhagens_ambitious_push_to_be_carbon_neutral_by_2025 (Last accessed Jan. 2, 2018).

[2] Rosslyn-Ballston Corridor—Projects & Planning—Arlington County. https://projects.arlingtonva.us/planning/smart-growth/rosslyn-ballston-corridor (Last accessed Jan. 2, 2018).

[3] Arlington County Energy Plan, Adopted June 2013 https://environment.arlingtonva.us/energy/community-energy-plan-cep/.

© Springer International Publishing AG, part of Springer Nature 2019

J. N. Pelton, I. B. Singh, *Smart Cities of Today and Tomorrow*,
https://doi.org/10.1007/978-3-319-95822-4_5

much better than a community that vacillates and flirts with one goal and another without achieving success in any of its objectives. Capricious and arbitrary goals that are never realized represent a recipe for failure.

If smart and focused planning on longer term goals with a sustained commitment is "king" of smart city development, then use of intelligent data that allows big data to be applied to a refined cause and effect model is the "queen" of truly effective urban planning.

This chapter explores the magic of effective use of big data that is analyzed within the context of proven causal models that can convert big data to intelligent data.[4] These are models that suggest how vital services, infrastructure, and drivers of change, such as demographics, tax base, etc., interact together to produce results. If one applies intelligent data (i.e., big data that is channeled and carefully analyzed within causal models) it can help measure rates of change and reveal which trends drive or influence others.

Does better education and health care improve a city's tax base or not? Does too rapid population growth strangle a city's chances for significant improvements? In light of limited financial and human resources, which investments are the right ones when hard earned tax money is available to be spent? These are types of questions that intelligent data analytics can answer. The key here is to examine large flows of data within the appropriate causal model so that you can find answers to key questions such as where investments will produce the best returns, based on what has worked and what has not produced positive results.

Intelligent data and clear causal model analysis can reveal to urban planners important trend lines. This analysis can honestly reveal where you are today, where you are going, and how fast you can expect to get there. A simple and very straightforward example is Arlington County, whose officials have been measuring CO_2 parts per million in its atmosphere over time to assess energy efficiency. Arlington County is using this data as an index as to whether its energy efficient program is proving successful. The goal of this energy plan instituted by the Arlington County community is to install and use sustainable energy sources more and more. It is believed that if this plan is followed consistently for decades it will serve to reduce dependence on coal and petroleum-based energy supplies, clean up the atmosphere, and create a more sustainable and livable community. The objective measurement of carbon-based gases in the atmosphere serves as a useful quantitative measurement device to see what progress is being made. In many cases causal models are multi-dimensional. The causal model shown in Fig. 3.1, as developed by the DataMi

[4] "Smart Data" and its meaning is critical to understand. This is a concept similar to big data but with greater focus on key interactive variables. This is a type of analysis that is still conducted using large data streams, but in this case the focus is not so much on volume, velocity or variety. Instead the attempt is made to create interactive models of behavior and systems operations. This focus can help identify the most valuable data to interpret. It can show the results that come from changing the interactions between and among major forces of change. This use of analytics, artificial intelligence, and heuristic algorithms that operate within a known system of interactive drivers allow the identification of what is the indeed the key data that is "valuable" and the importance of confirming that the data is accurate, unadulterated and thus verified.

Corporation, has more than ten different drivers of change and causation, and thus the study of how these various aspects interact depends on analysis of many different big data stream sources to identify what is cause and effect. There is always a danger of not identifying intervening variables and sorting out what are the fundamental forces of change.

This chapter seeks to explain the power of analytic tools that can help city officials and planners understand how the various forces of change truly interact and which have the greatest effect. By using smart city planning and investment tools based on intelligent data analytics, cities can make more cost-effective investment decisions and mitigate investment risks.

Developing Realistic Models That Can Be Scientifically Measured

The analysis of big data has become a very hot and popular field. In a very straightforward area, such as looking at the performance of a professional tennis player, it is possible to examine such factors as difference in performance levels between wins and losses. If after looking at data from hundreds of matches it might be found that the player won 70% of first service points in successful games but only 57% of first service points in losing games. This might suggest to tennis coaches to concentrate on service techniques. The point is that when the equations are straightforward to test performance against various factors such as 1st service success, 2nd service success, forced and unforced errors, performance at the net, etc., the running of the data without specific criteria can still produce useful results. In the case of urban design with a large amount of complementary and even conflicting variables, analysis without some plausible causal models of how key drivers interact, running big data through high speed processors is likely to be mining very low grade results.

The key is to develop plausible causal relationship models and then to examine big data streams that either reveal the extent to which these relationships exist—or not. The following causal relationships diagram (see Fig. 5.1) represents one such causal relationship model. This simple Bayesian network seeks to show causal relationships between various parts of an interactive network that might operate within a smart city's key functions.

This is not intended to be a complete representation of all the functional parts of a city, because such a model would be too complex to be easily understood. The purpose of this model is to suggest that the following relationships exist: (a) that schools, education and training support the creation and sustaining of jobs; (b) that jobs and the salaries that they generate supports the tax base of a city; (c) that schools, education and training support public safety; (d) that cybersecurity supports schools, public safety, health care, the tax base, and quality of life; (e) that jobs and zoning also support the tax base; and (f) that public safety support jobs, schools, health care and quality of life.

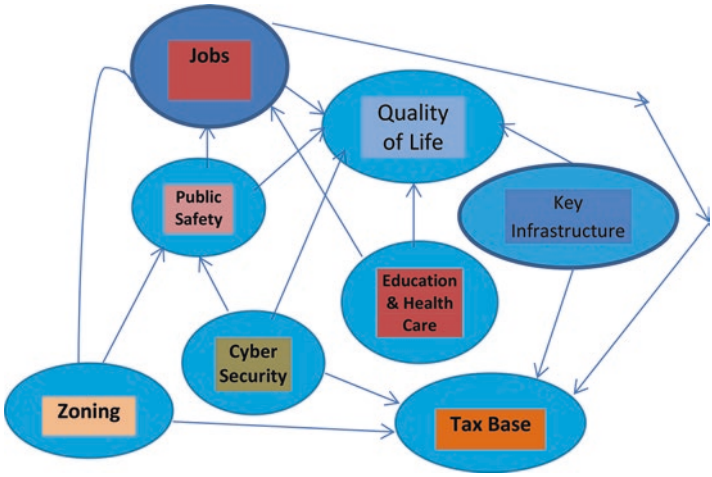

Fig. 5.1 A simplified Bayesian network diagram of key components within a smart city

Of course, the tax base directly or indirectly supports all of these urban elements. Indeed, if all of these elements are well organized and operate effectively and efficiently they support, at least indirectly, all of the other elements. The purpose of such a chart is to find prime causal relationships and to see if historical empirical data support the findings and the importance of these relationships. It is also to see how these changes are instituted so that these causal relationships might be strengthened. One of the key questions is whether the strength and degree of these relationships change over time as key factors such as demographics shift. If the average age of a city grows older are there changes needed to the schools, educational and training systems, the health care system, or perhaps the transportation system? In the diagram below neither transportation, energy, nor environment are depicted, simply to make the diagram less complex. The idea is to develop likely causal relationships and then look for data that supports the hypothesis and especially to look for new insights by running these models against actual historical data. Table 5.1 summarizes the particular advantages of causal analysis as opposed to conventional big data analysis.

The assumption is that historical information in the form of big data does not lie. But in truth there can be what are called intervening variables. This means that X causes Y and Y in turn causes Z. This might lead one to conclude that X causes Z, when in fact it is Y that causes Z. Causal models such as in the Bayesian model above allows the exploration of cause and effect for many things over time. Once cause and effect are properly sorted, then it becomes possible to examine key "what if" scenarios over time.

If a community's average age becomes older, does this mean that there is a need for more taxi and Uber services and less ridership of public transit? Does it mean that younger people need to be recruited from other areas to fill job openings? Does demand for types of housing change? What does it mean for school enrollment and ongoing educational offerings for adults and the elderly?

Table 5.1 The important strengths of intelligent causal analysis in urban planning

The Strength of Intelligent Causal Analysis[a]
• It is good at spotting patterns, clusters, associations
• It identifies and quantifies strength of associations
• It assists in predicting some further observations from other patterns
• It assists in showing how much one variable can change another

[a]Key points presented by Data Mi Corporation to characterize advantages of intelligent causal analysis in relationship to brute big data runs of large datasets

What is the impact if the average age of the population becomes younger and transient? This might represent the profile of a high-tech area where younger people spend more time at work, eating out and engaging in recreational pursuits and less time in their apartments or condos and moving from one job to another and switching housing. For such a community profile there will likely be a need to adapt to changing needs in the schools and educational and health care systems, public safety services, housing, and master planning as to what type of infrastructure to plan for and build.

The key to this type of longer-term planning and analysis is not to create processes to mold the city's population to meet the anticipated future needs of the community. Rather it is to create a city that can respond to the future needs of its evolving population and make the community a better place to live, work and raise a family. A planning process that ends up "selling" technology may well end up with the wrong type of infrastructure or wrong type of vital city services. This is of course a symbiotic relationship where the people and businesses of the city must indicate their current and future needs, while city planners solicit and seek to anticipate future needs.

The best of all possible worlds in a smart city is a situation where the citizenry, businesses and urban planners are united in their efforts to create an inviting community that retains its best and brightest talents and becomes a better place to live. This can best be attained when everyone involved seeks to create an ongoing political and economic climate that encourages positive organic growth toward a core value of creating a better quality of life for all concerned. In all of these regards causal analytics can be a useful predictive tool. These casual analyses or predictive analysis techniques are good to detect cause and effect relationships. They can help to identify key drivers of change. This can, in turn, allow city officials to adjust plans in order to create a better urban environment, make smarter investments, and

Table 5.2 Strengths of causal analysis as applied to "Big Data" processing

Causal Analytics Are Good For:
• Capturing complex interactions between forces that cause something to change—for the better or worse.
• Quantifying strength of associations and cause and effect relationships among and between key drivers.
• Predicting outcomes by analysis and processing historical big data that are applied to causal analytic models and Bayesian diagrams.
• Predictive modeling of the impacts that are likely by altering controllable variables.

provide a higher quality of life. The strengths of causal analysis are summarized in Table 5.2.[5]

This use of Bayesian diagrams, creating causal models, and predictive modeling of outcomes by altering controllable variables, of course, starts to sound incredibly complicated, and skeptics may well begin to say: "Wait a minute. Show me some practical results in the real world."

How to Avoid Dumb Mistakes and Create a Truly Smart City

Converting the "theory" of causal analysis in terms of smart city planning into practical use that really works is of course the true challenge. As always, as the old saying goes: "the proof is in the pudding." This means you might have a great recipe, but if the dish you actually fix is terrible, then who really cares. Bad results are bad results, period.

The mystique around smart cities as a very current hot topic is that the right combination of new technology, such as broadband communications, clever use of sensors, AI, automation and robotics, can make cities more effective, run smoother, cost less to operate, and safer. But the mindless installation and use of technology without considering its impacts and potentially counterproductive results is a big mistake. Causal analysis and predictive modeling can save a lot of time, grief and missteps along the way.

Case Study in Public Safety: Using Causal Analysis on a Small Scale to Install Robotic Guards in the City

Let's consider some case studies where causal analysis and the use of intelligent data might produce useful results. In San Francisco, California, the Society for the Prevention of Cruelty to Animals (SPCA) had been having a problem with building and car

[5] Stephen L. Morgan and Christopher Winship, *Counterfactuals and Causal Inference: Methods and Principles for Social Research* (2nd Edition) (2015) Cambridge University Press, New York.

break-ins, vandalism, petty assaults and harassment of its employees. The decision was to enter into a contractual arrangement with the robotics company, Knightscope, to have a 400-pound (180-kg) robot roll about on evening patrol along the sidewalk and across the parking lot of the SPCA facility. This robot, model K-9 Autonomous Data Machine, rentable at $6 an hour, was programmed to take a rapid number of photographs of anyone it encountered. It was programmed to record security footage and notify police and SPCA officials if there were indications of a break-in or vandalism.

This activity by the SPCA turned out to be short-lived. The robot was reportedly attacked by barbeque sauce, feces, covered by a tarp and almost toppled over. The local and then national press reported on what seemed to be a war between K-9 and neighborhood homeless people living in the Mission District of San Francisco. The magazine *Newsweek* reported the incidents under the headline "Robot wages war on the homeless." This led to a storm of protest on social media, and the SPCA gave up the robotic patrolling. In Washington, D. C., in the area along the Potomac River known as Washington Harbor, a Knightscope K-5 robot known in this neighborhood area as "Steve" was pushed into the fountain area and had to be replaced by another robot that ended up with the more endearing name of Rosie.[6]

The point is that in this case it would have been wise of the SPCA to have done more research into the K-9 robotic patrolling system approach. They might have undertaken a critical review of alternative sensor technologies in countries such as the United Kingdom and cities such as New York City. They might have consulted the local community to have determined their response to patrolling robo-cops. Further they might have considered what other communities have done to cope with similar problems and even the cost of the Knightscope systems over time. This could have been done with a modest-type causal analysis or predictive analysis process. This analysis and modeling would have likely shown that an alternative and less overt approach with concealed surveillance cameras would have likely produced better results in terms of public safety, lower costs of operation, and certainly less hostile public demonstrations and negative press.

The above example of analytic evaluation of public safety is a quite targeted and limited example. There are, however, much more challenging issues that might be analyzed in the hope of discovering cause and effect relationships and important trends that might affect the future in important ways.

Case Study of Climate Change Effects on Migration: Using Causal Analysis on a Large Scale

There was a recent scientific study by professors at Columbia University published in the respected journal *Science*. This massive review of human migration examined the correlation of changes in the annual temperature shifts in over 100 countries and

[6] Peter Holley, "Accused of targeting the homeless, robot sees crime-fighting career cut short", *Washington Post*, December 28, 2017, p. A3.

then sought to determine the impact that climate change might have had on applications for asylum within European countries. This review covered the period that started in 2000 and ended in 2014. Their research found that there was a statistically meaningful relationship between migration and abnormal temperature fluctuations, which could also be linked to agricultural productivity. The study posits that these temperature fluctuations led to increased requests for asylum in Europe. The fluctuations encompassed only about 10% of the 325,000 sanctuary seekers per year during this 15-year period, but the researchers still found this correlation pattern was statistically significant.

Separate studies of temperature and other climate change variations in the Mesopotamia region, had previously examined migration during the period 2007–2010, and, amid some controversy, also suggested that these type temperature shifts were partially responsible for the disruptions in the area, particularly in Syria. Other studies that have examined drought in the Sahel region have again concluded that millions of residents had been forced to migrate, with many of them seeking sanctuary in Europe.

The interesting conclusion of the latest study by the researchers was to suggest that there was evidence not only of an increase in those seeking sanctuary in Europe, in response to dips in agricultural productivity due to rain and temperature variations, but that this was a strong predictor of future actions. Thus, Columbia researchers Schlenker and Missirian have, amid some controversy, suggested that they could project future migration trends based on the degree of the temperature change.[7] Accurate projections still remain uncertain, but there are now many other researchers seeking to correlate climate change factors to impacts on migration, seeking of sanctuary, agricultural productivity and economic prosperity or recession. Michael Werz, who is a researcher of this topic at the Center for American Progress, has indicated that climate change is relevant but not the only key predictor of migratory patterns: "It is one important piece of the puzzle, but it's not the only one."[8]

The above two examples of causal analysis to anticipate future impacts on cities represent the range of such activities. One study of a very specific issue involving public safety and the use of automation (i.e., in this case patrolling robots) is very specific and narrowly defined. The other issue involves a much broader issue, with the potential action of millions of people over many years, and is a much, much broader and more significant study, with the causal analytics much less scientifically refined. Most cases of such causal analysis to which intelligent data might be applied will be somewhere within this range of scientific definition and clarity of prediction of likely outcomes.

Many people know of the game known as *SimCity* that was launched to much acclaim in 1987 and has evolved into a number of electronic games since. Despite

[7] Chris Mooney and Brady Dennis, "Researchers project climate change will exacerbate Europe's migrant crises," *Washington Post,* December 28, 2017, P. A3.

[8] Tom Daschle and Michael Werz, "Food Security and Climate Change. New Frontiers in International Security." April 12, 2016, https://cdn.americanprogress.org/wp-content/uploads/2016/04/11113536/FoodSecurity-brief-04.12.16.pdf.

the disappointing launch of *SimCity 5* and Entertainment Arts pulling the plug in 2015 on the series, there are still many devotees to this educational computer game that explores the many conflicting demands to create a successful and vibrant city. The *SimCity* games allow participants to play out a series of decisions about zoning, development, taxation, etc., to see the likely—and unexpected—consequences of the decisions.[9]

To an extent causal analysis using intelligent data analytics is like a refinement of the methodology used in this popular game to examine how various aspects of a city's development are interconnected. The above study related to climate change and migration illustrates that a smart city planning and analysis must not only consider internal aspects of infrastructure, services, jobs and taxation within a city but external factors such as national taxation policies, migration into a country or city, etc.

Example of Designing a Smart City Using Causal Analysis and Intelligent Data

There are so many variables that can impact the planning, financing, implementation and operation of smart city. The options are rather overwhelming, and this makes it difficult for a city or an urban planner to know where to begin. There is no single right answer to how a predictive or causal analysis is done. There are many possible aspects to cover, options to evaluate, and potential datasets to process against models that can be created. Nevertheless, the following illustrative example provided here shows a generic set of issues and questions to address and the types of vital intelligent data that would be needed to chart the right course to create, implement and operate a smart city.

What must always be considered is that a smart city is more than a skyline or shiny new infrastructure (as suggested in Fig. 5.2). No, a smart city is one that is constantly improving to provide a better quality of life for its citizens and where there is a smart planning process in place where citizens can actively shape that vision of the future in partnership with a city's political leadership and committed urban work force.

The following approach to causal and predictive analytics as developed and copyrighted by the DataMi Corporation illustrates the steps that can be undertaken to evaluate options in urban planning.

The generic steps that might be employed in a causal analysis are first outlined in the initial Phases 0, 1 and 2 associated with a new undertaking. (See Fig. 5.3.) These steps are key to developing a Bayesian diagram for the critical Phase 3 analysis that follows. The first three phases identify some of the key questions to be addressed in developing a new approach for the design a smart city and the datasets that can be processed and analyzed in the key Phase 3 analysis. Figure 5.4 outlines

[9] Erik Kain, " SimCity' Developer Shut Down By EA" Forbes, May 4, 2015. https://www.forbes.com/sites/erikkain/2015/03/04/simcity-developer-shut-down-by-ea/#4ead1f362637

Fig. 5.2 A smart city depends on intelligent planning for improving quality of life (Illustration courtesy of Data Mi Corporation.)

the key aspects of the Phase 3 analysis. This Phase 3 analytical process seeks to identify interactive relationships and clarify how key drivers of change relate to each other when measured by actual data-driven indicators.

The technical details related to predictive analytics and causal analytics are complex enough to make one's head hurt. Sophisticated tools such as CAT (causal analytic tool) that has been developed by Cox Associates with support from the George Washington University Regulatory Studies Center are an extension of *Excel* that is available to Microsoft users. This can simplify the analysis of datasets that were set up on the basis of *Excel.* The purpose of this chapter is not to school those seeking to engage in predictive analytics or causal analytics. Rather it is to explain that there are competent consulting companies that can help define options and investment alternatives and employ data available to a city from past practices to evaluate the best steps forward.

It is useful, however, to distinguish the difference between the quite similar terms of predictive analytics and causal analytics and how these tools can be useful.

Predictive analytics can be defined as the practice of extracting information from past recorded performance datasets. This means that relevant historical big data that is available to a city can be used for analytic purposes. These datasets are processed using appropriate algorithms in order to determine patterns and to assist with more accurate predictions of future outcomes and trends based on past performance. Predictive analytics do not pretend to reveal the future but can provide a good context to determine past patterns of behavior. Such analysis where correlated with other data might help reveal why patterns were manifested in such statistics as rates

Phase 0 – Understanding the City, its Economics, and Other Key Influences for Change
What is the status of the cty or town?
Is it growing, largely stable, or in economic, cultural or social decline?
Young population, well distributed population, or aging population?
What are the top issues? (i) industry shifts and jobs; (ii) economic shifts and tax base; (iii) environmental/climate shifts; (iv)technology shifts; (v) public safety and crime; (vi) other.
What issues will be coming up in the near term and what issues should be addressed now to mitigate what needs to be done for long term vitality?
What dictates certain strategic choices, i.e., what are the key motivations?

A natural application of advanced decision analytics and models would be to identify the factors that affect choice of economic and community development, such as using the change that is occurring in the world economy to strategic advantage by making informed and collective decisions. Analyzing the choices then would help weigh the different factors, ranging from public actions, costs and impacts. This would help identify the probabilities of success by choosing among key options. Standard models in economic development use parametric regression techniques such as logistic regression to look at the relationship of demographics to current economic and social activity. Better results can come from using non-parametric methods based on dynamic analytics to show influencing factors for making a decision and what different paths should be evaluated. The results would affect everything from marketing, capital improvements, operations and funding streams.

Phase 1: Understanding and Visibility – the need to know where you are then where to go. Data: identifying data that is available and relevant to the issue at hand? (i) demographic data; (ii) budgets & expenditures; (iii) economic data for industries of interest; (iv) employment and automation trends; (v) infrastructure data; (vi) climate, weather, & pollution data; (viii) education, schools and training data; (ix) health statistics and health services data; (x) citizen surveys & public engagement; (xi) other

Phase: Analysis
a. What motivates the community to make new investments?
i. Look at situational factors – climate change and environmental factors
ii. Other reasons for choice – technology, historical processes, geography, cyber investments
iii. Changes in demographics
iv. Changes in community behavior. What are the new values for the community?
3. Decision support factors and tools
a. When they spend funds, what are the most likely impacts on key variables?
b. Are they making the best decisions given limited funds?
c. What do they need for various operational and capital improvement decisions?
d. Decision support tool and CAT analysis to help with "What If?" analysis

Note: At the end of phase 0 it is also possible for items 1 and 2 to be completed. This would lead to the critical Phase 3 analysis. This analysis process would need to involve, on an active basis, various city departments. It would also involve developing agreed key Bayesian diagrams. Once this is complete then the stage is set to undertake the Phase 3 smart data analysis. (Provided by one time license agreement from the DataMi Corporation, who holds copyright.)

Fig. 5.3 Generic approach to causal analysis using smart data

Phase 3– Decision Support Factors and Tools:
Causal Analysis Based on Agreed Bayesian Diagrams and Processing of Smart Data

a. When and where to spend funds that are the most likely to impact key variables?
b. What are the best decisions that can be made given limited funds?
c. What key inputs are needed for various operational and capital improvement decisions?
d. What level of community support is needed for key decisions, and how is this developed?
e. How can the best decision-support tools be developed to help with "what if?" analysis

The answers to the above questions can be developed using causal analysis and smart data that has been identified as critical to decision making such as.

1. **Operational decisions:** These must be fitted to a city's decision-making processes, schedules, and related dynamics
2. **Capital investment decisions:** Where to invest? What type of investments to make? Is it of a special type such as some form of public investment? Some special form of muni-bonds? Paygo? Other forms of financing?
3. **Capital sources**
4. **Staffing and technical support and contractors**
5. **Public safety and cybersecurity**
6. **Behavior nudges and campaigns**

This analysis should identify the factors that most affect choice of public investment spending, such as roads vs. fiber optics (i.e., physical infrastructure vs. intellectual infrastructure). This requires analysis and quantifying different factors. These factors range from types and number of jobs to services, type of infrastructure, etc. It assesses the probabilities of choosing the best investment and the future impacts on a community. Standard models in economic and city planning use parametric regression techniques such as logistic regression. Causal and predictive correlations that go to the environmental , financial, zoning, employment or other causal factors that will make a long-term difference in defining longer term goals and decisions as to how to invest in infrastructure, how to concentrate development, how to finance improvements, and much more.
.

Fig. 5.4 Key aspects of Phase 3 analysis in 'Smart City' planning (Provided by one-time license agreement from the DataMi Corporation, who holds copyright.)

of building of new housing or commercial properties, increases in pollution levels, or increased rates of water usage.

Causal analytics is a very similar concept to predictive analytics. The main difference is that it tends to create more complex cause and effect interrelationship models with regard to a larger number of drivers of change that might interact to influence one another in a more complex manner. The risk of more complex models is that they tend to make too many assumptions. If models are overly complex they can misinterpret the nature of urban interactions. This could lead to identifying false relationships between two or more drivers of change. Such false relationships are typically called "intervening variables" by scientists. (An example would be an instance where two men frequent a bar and both came home with colds. The presumption might be that they both caught the cold in that bar. The true cause was that

the two men had also visited a brothel where a prostitute had a bad cold. The men confessed to being at the bar but not having been to the brothel. This lack of accurate or complete data can conceal the true cause and misidentify the source of the cold as being the bar rather than the brothel.)

The whole point of both predictive analytics and causal analytics is to process big data in a more intelligent way so as to reveal meaningful interactions and correlations as clearly as possible. Instead of just processing data without any preset models or structure with the hope that a pattern or meaningful conclusion will emerge, predictive analytics and causal analytics posits that relations should likely exist and then runs historical big datasets that are available to see if such patterns are indeed there. This process can transform so-called big data into intelligent data analytics.

Conclusions

The most prosperous large cities with well-established tax bases are, in some instances, inclined to invest in the latest technologies and create what seem to be the most modern cities in terms of broadband telecommunications and networking systems, the fastest and most automated transportation systems, and communities that are energy efficient and "sustainable" from an environmental perspective. Such efforts to modernize infrastructure and automate systems may well represent wise investment and attract the most productive industries and wealthiest citizenry to sustain continued growth and development. However, a smart city is more than shiny new technology and the latest shiny gizmos driven by artificial intelligence.

A smart city has inclusive political processes that strive toward a vision of ongoing improvement. This allows citizens, businesses, volunteers and city planners to work together to create a community that is more livable and responsive to the needs of both its citizenry and business community. The goal is to achieve an improved urban vision through causal data analytics. If done well it can help to identify wiser investment, better choices for technology upgrades, or where new staff or training can realize the most bang for the buck. Here are some of the areas where causal data analytics might produce useful results.

- More sustainable energy and transportation systems, or faster progress toward a zero-carbon footprint and the control of pollutants.
- Improved quality education and health care services.
- A more vibrant business community, development of new business enterprises, job growth or development of a growing tax base.
- A better balance in sources of tax revenues from multiple sources.
- More livable and affordable viable housing, better utilized parks and recreation systems, or new opportunities for the pursuit of happiness.
- Optimized public safety systems designed to cope with natural disasters, criminal activities, terrorism, and cyber-attacks.

- Modernized and perhaps more automated infrastructure that are better-protected by cybersecurity systems and also designed to accommodate growth and cope with limits foreseen by predictive analytics.
- Planning process to avoid dangers of super-density by control of growth and encouraging the development of meta-cities and tele-commuting systems to preserve public safety and livability.

Each city exists within a national economic, political, cultural, ethnic and business environment that creates both constraints and opportunities. Immediately after World War II in 1945, Japan, China and most European countries had been devastated by war, and their cities and infrastructure were in ruins. Today these countries, their economies, their public services and their infrastructure, housing, and businesses have all recovered. This result is in part due to hard work and steady recovery, and in part due to planning with vision to make their cities more livable and prosperous. This chapter is about many things. It is about recognizing problems and analyzing how they might best be addressed through the sophisticated planning tools now available. It is essential to recognize the vital importance of short, medium and longer-term planning that is driven by a clear vision.

A key part of that planning process is setting clear goals for the future and having a vision of what to aspire to in future years. Another part of the process is to examine alternatives, identifying patterns of behavior and constraints that need to be removed to accomplish goals. This process must always recognize that the citizenry and the business community have to be directly involved in and supportive of this urban planning process. Tools such as intelligent data analytics, predictive analysis and causal analyses are just tools. Such tools in the wrong hands and badly used will produce bad results. Unless there are clear goals backed by good and competent government, and broad community support, they will almost certainly be ensured to fail. A strong, clear, forward-looking vision of what a community aspires to become is the first step to community progress, but then the hard work of making positive steps toward those goals begins. Changing demographics, overpopulation and super-density, pollution, climate change, the threats of chemical, biological and nuclear weapons, and adapting jobs and employment to a new world of automation and autonomous networks are all difficult challenges.

In the age of smart cities cyber-defense must be added to this list of threats to urban societies. These urban threats to the world of smart cities are particularly challenging because the pace of change is so very fast. In the age of the Industrial Revolution in the United States, some seven million workers had on the order of 50–70 years (i.e., three generations) to shift from farming and mining to working in industrial jobs. In the case of the shift of industrial to service jobs in the United States the number of workers that shifted their careers and professions involved many more people in a much shorter period of time. In the age of automation, what might be called the “Fourth Wave,” the shift again involves more people switching at an ever-faster pace and the nature of these new occupations is far from clear. Addressing such problems is part of the visioning process. Analytics must help us consider the best options.

A world with some 10–12 billion people, as we will be at the end of the 21st century, is a much more complicated and difficult one than when our small planet had a population ten times less. Planning and accommodation to change is a task that is in many ways ten times harder that it was a century or two ago. The complication of automation, cyber-networks, and cyber-attacks and techno-terrorism represents a much greater threat to society than many people now understand.

There is also a danger in making forward-looking decisions based entirely on historical data. A study by Mercedes Benz has projected that a future with autonomously driven cars will allow people not to own cars and to have an accident only every 6 million km driven instead of every 60,000 km. This study, for instance, projects the following: "In 2018 the first self-driving cars will appear for the public. Around 2020, the complete industry will start to be disrupted. You don't want to own a car anymore. You will call a car with your phone, it will show up at your location and drive you to your destination. You will not need to park it; you only pay for the driven distance and you can be productive while driving. Our kids will never get a driver's license and will never own a car. It will change the cities, because we will need 90-95% fewer cars for that. We can transform former parking spaces into parks."

Our modern world is also much more exposed to cosmic hazards such as asteroids and near-Earth objects, solar storms, and changes to the world's magnetosphere than ever before. This is because of a huge and growing population that is ever more dependent on electronic grids, modern transportation and communications systems, and automation. It is only after losing these vital infrastructure facilities that the extent of our dependence would be dramatically apparent. The use of modeling tools to assess key what-if and what then'" questions can help us plan for the future and create smart cities that are indeed smarter, safer and more viable. No one can predict the future with accuracy, but the planning tools introduced in this chapter can help us chart a better way forward.

As a final note, some readers might be saying at this point that this type of fancy computer analysis might be fine for a wealthy city with lots of computer nerds and resources, but this is not something we can do in our own town. What about us? One possible answer is to learn from the shared experience of others and benefit from some of the findings and experiences of other towns and cities. The brief addendum to this chapter provides some useful insights from cities and towns that have examined problems, exploited opportunities, or diagnosed ways to make their community better. Some of these positive results came from recent intelligent causal analytics and others came from old fashioned civic planning processes fueled by citizen support and creative leadership. These ideas might work in your community.

Addendum

Smart Planning in Urban Design and Use of Causal Analytics Verification

1. **Bull's Eye Development Around Metro Stops in Arlington County, Virginia:** Dr. Joseph Wholey, Chairman of the Arlington County Board and a staff member of the Urban Institute, used relevant causal analytics research from around the country to lead a Long Range County Improvement Commission to develop a long-term redevelopment plan for the so-called Rosslyn-Ballston Corridor. This plan called for new development to concentrate "mixed-use" (residential, commercial, retail and office development) in high-rise development around new metro system rapid transit stops. The resulting shift for the R-B corridor between the 1970s and 2018 was to increase office space development (from 5.5 million sq. ft. to 23 million sq. ft. or a factor of 4) residential units (from 7000 to 33,500 units or a factor of 4.5) and retail commercial (from under 900,000 sq. ft. to 3.2 million sq. ft. or a factor of 3.5) and jobs (from 22,000 to 90,000, or over a factor of 4). Today Arlington has 85% of its concentrated development in under 15% of county's limited area. Its tax base is evenly matched between residential development and commercial development tax revenues. This commercial development in the R-B corridor and Crystal City area (also a metro corridor) has generated urban financing that has allowed the creation of an extensive park and recreation system and a public school system that is rated as one of the best in the United States. The mixed-use development has created a lively urban environment where people live, shop, work and enjoy food and entertainment 24 hours a day with easy access to metro transportation. (Source: Presentation at public Digital Destiny forum in Arlington, Va., by Robert Duffy and Joseph N. Pelton, March 14, 2018.)
2. **The Creation of Special Interest Sector Focus in the Smart City of Dubai.** Urban planners in Dubai wanted to create a special appeal for their efforts to attract new talent and capabilities to the city-state Emirate of Dubai. They brought in urban planners to help them share their aspirations with the world community. These consultants indicated that an exciting new city had to offer more than money and financial incentives. The concept was to divide the city into sectors that focused on particular capabilities and interests. Thus the "New Dubai" would have featured capabilities and interest. There would be a Dubai University city sector, a Dubai for health and medical services, a Dubai for banking and financial services, a Dubai for broadband and IT industries and so on. Each of these sectors would have special recognition, branding, and infrastructure with services and facilities geared to the needs of professionals and companies operating in their sector of interest. This idea of creating exciting "cities" within a city with special thought to their needs, interests, and professional requirements proved to be magnetic to the planning and modernization of the

Dubai smart city as it has been re-envisioned and deployed over the past three decades. This has included a combination of exciting architecture, high-quality infrastructure, and recruitment of world-class organizations that wish to partner, associate, collaborate, or even compete with the best capabilities from around the world. This program has proved to be highly successful, but this very success has created new challenges in that the cost of living and the cost of real estate in Dubai have become quite expensive. (Source: Dr. Indu Singh, who helped develop these concepts.)

3. **Smart Transportation Systems and Measured Performance Improvements.** Smart transportation systems continue to be implemented and performance improvements measured in a variety of ways. The smart signal adaptive traffic control system that Carnegie Mellon University has developed has been implemented in many cities, including Chicago and Singapore, with typical improvements in wait times being reduced by around 40% and rush-hour travel times reduced by around 25 after implementation. This system, known as SURTRAC, is only one of this type of system that uses smart traffic signals to monitor the flow of vehicles and develops algorithms to speed traffic efficiencies. Other systems have registered similar efficiency gains with similar use of smart traffic signals to monitor traffic flows in other urban centers. Other capabilities to allow vehicle-to-vehicle communications to monitor and improve traffic flows and reduce accidents are now under development, such as the Safe Pilot Model Deployment system that is being tested in Ann Arbor, Michigan, under research funding from the U. S. Department of Transportation. (Source: Shawn Dubravac, Digital Destiny, (2015) Regnery Publishing, Washington, D. C.)

Chapter 6
Protecting Privacy from Internet Abuses in the Smart City

Digital technology and artificial intelligence in the smart city can do a lot of good things, right? You'd better believe it!

These powerful technologies and software can advance the efficiency of operations and services, reduce staffing requirements and costs, improve tax collection effectiveness, and aid public safety. They can be powerful tools against crime and terrorism.

However, there can be downsides. Abuse of privacy, governmental snooping into people's private lives, and even illegal monitoring of political behavior can lead to the suppression of citizens' rights. Electronic monitoring can lead to the loss of freedom and liberties and suppress the citizenry's expression of political viewpoints. Further, as seen in political elections in Europe, Taiwan and perhaps most notably in the U. S. presidential election of 2016, outside interests and foreign governments can use social media to promulgate false or distorted information. The use of bots as "trolls" to seek to manipulate elections represents a very specific concern that emerged from Russian intrusions into the 2016 U. S. presidential elections and in a number of European countries from the United Kingdom and France to Hungary and the Ukraine.

And there is also the very real problem that some young people seem to live their lives on social media. Educators are now seriously concerned about the overuse of social media and even what might be called Internet addiction. In the United States organizations such as Jana Partners and the California State Teachers Retirement Fund, which together control $2 billion in Apple stock, have asked Apple to convene a committee of experts to see what more can be done to control this. There is particular concern about the dangers that can come from overuse of smart phones by young people. Recent studies of this issue with regard to students in the United States have cited "a decrease in the ability to focus on educational tasks, difficulty with social interaction, loss of empathy, links to stress, and higher risks of depression and suicide."[1]

[1] "Helping children unplug" Washington Post, Jan.16, 2018, P. A16.

© Springer International Publishing AG, part of Springer Nature 2019

J. N. Pelton, I. B. Singh, *Smart Cities of Today and Tomorrow*,
https://doi.org/10.1007/978-3-319-95822-4_6

Industry respondents from Apple, Samsung, Facebook, and other social media businesses have noted the various parental controls that can be used to limit access and the use of social media, but clearly this is now a growing issue. And the problem is not restricted to students. Even going back 20 years there have been "Internet addiction centers" established in the state of California for people who have literally become addicted to Internet access and have as a result lost their jobs and their families as a result of being online virtually 24 hours a day.[2] Clearly parental controls as currently applied are not sufficient.

Can Misuse of the Internet Threaten Democracy and Free Elections?

Silicon Valley correspondent Elizabeth Dwoskin, in her *Washington Post* assessment of the likely big news for 2018 for the field of ICT technology, summed up these types of concerns thusly: "People worry that social media can be manipulated by foreign governments, poisoning democracy and tilting the outcomes of elections. They fear that software algorithms are fueling disinformation, censorship and hate speech. And they are concerned that tech giants have become powerful gatekeepers."[3]

It apparently is now common practice by nations to employ professional trolls and robotic sites to try to sway voter opinion one way or another and tilt elections in other countries. Some would even say that this unfettered use of social media could become a serious threat to democratic processes around the world. Buzzfeed, an online political reporting network in the United States reported in November 2016 that "top fake news reports online" had significantly larger impact in terms of measured face time over actual legitimate "factual news" during the presidential election. They reported that "engagement on Facebook" with 'fake news' as purveyed by bots and trolls exceeded in hits that of 19 legitimate news outlets combined.[4]

A detailed study of Hungary has found that there are 30 websites that are devoted to providing slanted information to targeted groups of Hungarians, and this activity is sufficient to form public opinion in a significant way in a country of this size and level of Internet usage. Other studies are now underway to find out the level of "attacks" via the Internet that are being carried out by external campaigns.

The bottom line is that at least several nations are today engaged in what can accurately be described as cyberwarfare against adversary nations. Democratic countries that explicitly provide by law and by constitutional guarantees for freedom

---

[2] Joseph N. Pelton, *e-Sphere: The Rise of the World-Wide Mind*, (2001) Bridgeport, Conn.: Quorum Press.

[3] Elizabeth Dwoskin, "Big tech will confront their dark side", Washington Post, December 31, 2017, p. B3.

[4] Zeynei Tufekci, "The [divisive, corrosive, democracy poisoning}Age of Free Speech" Wired Magazine, Feb, 2018, pp.

of speech are the most vulnerable to such attacks—especially via the anonymous platform that the Internet and social media now provides.

Smart city leaders, officials, and staff today are making extensive use of digital technologies to defend and protect against cyber-attacks by hackers and techno-terrorists and to fight crime. But it is a small step from these uses of digital technology to illegal snooping and suppression of rights. Thus, in democratic societies there are now growing concerns about the misuse of digital technology to undermine a citizen's right to privacy and even worse to threaten freedom, liberty and other core democratic principles.

As of late 2017 and early 2018 there was in the United States considerable discussion in the U. S. Congress about whether to extend, or water down, the provisions of the U. S. Foreign Intelligence Surveillance Act (FISA). This is the act that establishes a special FISA court that oversees the activities of the National Security Agency (NSA). The NSA is legally authorized to monitor conversations around the world to detect threats against the United States. This special court, under the FISA act, can also authorize surveillance of individuals inside the United States, including U. S. citizens, if the court officially deems that these citizens might be engaged in activities harmful to the United States.

In this particular case the issue of the renewal of the FISA act is apparently not so much about protecting the rights of U. S. citizens against unwarranted eavesdropping but rather involves members of Congress protecting revelations about activities by the members of the Trump campaign with regard to their possible collusion with Russian officials' interference into the U. S. 2016 presidential election. In short, the concerns were less about protecting U. S. citizen rights and more about preventing the "unmasking" of the identities of officials involved in these activities by the Trump campaign.[5]

Certainly, the concern about electronic surveillance, both legal and illegal, as well as attacks on the free press that revealed these abuses is not new in the United States. Indeed, it was one of the key issues in the United States during the Nixon Administration. Many details of abuses were revealed during the Nixon impeachment hearings. A furor arose when it became known that President Richard Nixon had an "enemies list" and that he had commissioned illegal wiretapping, Internal Revenue Service audits of "enemies," and even obtaining of electronic messages by illicit means from telecommunications carriers. Illegal snooping and orchestrated attacks on the free press that came out in the Watergate hearings showed that such issues were not limited to totalitarian states, but that the United States and other democracies were vulnerable as well.[6]

And indeed, history in some ways seems to be repeating itself. Omarosa Mauigault, who was head of African American outreach in the Trump campaign, was quoted as saying during the Trump campaign: "Let me just tell you, Mr. Trump has a long memory, and we're keeping a list."[7]

---

[5] Karoun Demirjian, "Key NSA surveillance program's reauthorization stalls in Congress, Washington Post, December 21, 2017.

[6] John Avalon, "How Nixon's Hatred of the Press Led to His Downfall, The Daily Beast, Sept. 5, 2017 https://www.thedailybeast.com/how-nixons-hatred-of-the-press-led-to-his-downfall-5.

[7] Eugene Scott, "Omarosa: Trump Campaign Keeping an Enemies List" *CNN*, Nov. 9, 2016 http://

Why Smart City Planners Must Be Concerned About Abuses of Technology

Today, in country after country, concerns about privacy, surveillance and threats to liberty and freedom from electronic monitoring and "Big Brother" tactics have become a matter of serious concern. In the age of the Internet, rampant use of social media and ever more sophisticated use of electronic sensors, listening devices, and monitoring technology the story is clear. Individual privacy is under attack.

Some of the privacy concerns come from what start out as what city planners consider to be helpful ways to make their communities smarter and more responsive to citizen needs. There is a project in Toronto, Canada, that is installing a very intensive number of smart sensors. The project has been described in this manner: "It's being imagined as the sort of place where garbage cans and recycling bins can keep track of when and how often they're used, environmental probes can measure noise and pollution over time, and cameras can collect data to model and improve the flow of cars, people, buses and bikes throughout the day." When businesses and people in the neighborhood agree to the terms of city services they are in this new smart environment, also agreeing to being monitored in a great many types of ways.[8]

However, there are even more direct and intrusive types of surveillance now underway. Some governments have installed millions of surveillance cameras, installed facial recognition software to find people along city streets, and authorized the use of listening devices to eavesdrop on citizens' conversations. The latest innovation in what might be considered a form of political suppression is the monitoring of electronic usage practices by individuals. As noted later in this chapter China not only has its Xue Liang (i.e., "Sharp Eyes") of video surveillance expanding to cover the entire nation, but it is now creating a computer-based "rating" systems for all of its citizenry. The purpose of these "social credit scores" is presumably to assess the "loyalty" of citizens to their governmental dictates as they conduct their everyday lives. And this is not just a concern with regard to governmental snooping and oversight.

Online businesses, such as Ali Baba and other online retailers, are engaging in similar practices, presumably for commercial rather than political purposes. These concerns, with privacy and political monitoring and control of citizens, have grown sharply in the past decade. This is partially a result of advances in electronic and sensor monitoring technology that have suddenly spurted ahead. It also due to the feeling that political systems in the both the East and West have become increasingly more controlling—often as a result of anti-terrorism and organized crime defenses.

What is clear is that electronic systems have become more invasive. What was once only conceived in fiction, i.e., *1984* or *Brave New World*, or in science fiction movies, i.e., *Enemy of the State,* have now become true concerns about actual practices in both business and government. The investigation of the various outside

---

www.cnn.com/2016/11/09/politics/omarosa-list-donald-trump/index.html.

[8] Matthew Braga, "Welcome to the Neighbourbood" *CBC News*, Jan. 16, 2018 http://www.cbc.ca/news/technology/smart-cities-privacy-data-personal-information-sidewalk-1.4488145Math.

intrusions into the U. S. presidential election of 2016 has led to the revelation that 50 million personal records of Facebook users was released to a U. K.-based company known as Cambridge Analytica that then proceeded to "weaponize" this information aimed at affecting potential votes in the election.[9]

These findings regarding Cambridge Analytica have led to almost an avalanche of privacy concerns. Not only has Facebook's stock taken a hit, many have "unfriended" the company that had compromised their privacy and have closed their personal accounts. And privacy concerns have now spread to other companies such as Amazon, Google and Apple. A Gallup poll of the U. S. public has found that 22% of those now use home devices such as Google Home or Amazon Echo to answer questions, order products, activate home utilities or other data-related services. This means that information companies can create profiles of individuals or families by storing and tracking this information. And pending patents show that this is perhaps just the tip of the iceberg.

The president of Consumer Watchdog, Jamie Court, has been quoted in sounding an alarm thusly: "When you read parts of the applications, it's really spyware and a surveillance system meant to serve you up to advertisers." The bottom line is that as one uses a cell phone or accesses the Internet today, one should probably assume that all of our activity is being tracked—perhaps to find your tastes and spending habits, perhaps to learn your political views, or even to monitor suspected criminal behavior or crimes against the state by law enforcement agencies.[10]

This chapter explores what some of these practices actually are, governments and businesses that are engaging in installing and using this type technology, and possible constitutional, legal and regulatory practices to control the most egregious of these practices. Likewise, there are growing concerns about overuse of social media and Internet addiction that goes beyond concerns about the manipulation of public opinion and concerns that this can inhibit learning and lead to cyber-bullying, anti-social behavior, and even mental disorders—including depression and suicide.

As is always the case with regard to use of technology there are trade-offs to be made between useful and desirable ways to deploy technology and to prevent abuses that can arise from using that same technology.

Social Media and the Embracing of Sharing One's Life Styles, Especially by Millennial Youth

There are many ways that change can be measured in terms of things that are tangibles and quantitatively specific. The gross national product of France, the barrels of oil produced by Saudi Arabia in a year, or records sold by Beyoncé. Societal

[9] Marcello Ienca and Effy Vayena, "Cambridge Analytica and Online Manipulation". *Scientific American*, March 30, 2018, https://blogs.scientificamerican.com/observations/cambridge-analytica-and-online-manipulation/.

[10] Sapna Maheshwari, "Hey, Alexa, What Can You Hear? And what Will You Do with It?" New York Times, April 1, 2018. P. 1 and 20.

changes in behavior are much harder to chart. There is no doubt that younger people—so-called millennials, the Gen X, Y and Zers—i.e., those who grew up in the world of the Internet—have different attitudes about privacy and sharing of personal information. People born in the 1980s and after have learned to chat with Google's Siri and Amazon's Alexa and let it all hang out on social media sites. They generally relate to technology differently than older generations. There are startling examples of young people sexting, sharing illicit text messages and even displaying criminal acts on their Facebook site. Also, as noted earlier, there are concerns about Internet addiction.

There are a number of sociological studies that confirm that a significant number of millennials are comfortable with sharing quite personal information over the Internet. Tweens to 30-year-olds accept that in a broadband electronic world, privacy is generally not "expected" and often not greatly protected. A number of young people have lost out while interviewing for jobs because they have posted too explicit pictures or political opinions on their Facebook page, their blog or other social media. Here is a tip to the wise. It is best not to post pictures of yourselves while nude or drunk. Likewise, it is best not to post political diatribes or racial slurs on line. In fact, it might not be wise to engage in outrageous or anti-social behavior in the first place.

Systematic surveys by the Pew Research Institute and others have confirmed the fact that younger people have and do share more personal information that older people. This seems to reflect the recognition that there is much less privacy today because of the pervasiveness of electronic media and the inevitability of all sorts of information being widely shared (Fig. 6.1).[11]

In short, we live in an increasingly viral world. Many younger people do not see the problem so much as protecting privacy but actually getting their Facebook page and their personal blog recognized by an ever expanding group of friends and colleagues. This does not mean that younger people are indifferent to their privacy but rather seem to be more aware of the pervasiveness of personal information that is now available online even if they take steps to preserve their personal information. Other studies are now showing that overexposure to social media can lead to problems of learning, focus, and anti-social behavior.

What is not clear is the public perception of how much intrusion of privacy via various electronic means not only intrudes on people at a personal level but could threaten democratic principles and be used for systematic control of economic and political activities at the broad societal level. Monitoring and even "rating" of individuals via electronic media by commercial organizations, governments and other entities is becoming more and more pervasive. Detailed dossiers and individual profiling is now not only possible but is a trend growing around the world.

[11] Lee Rainie, Sara Kiesler, Ruogu Kang and Mary Madden, "Part 2: Concerns About Personal Information Online", September 5, 2013 http://www.pewinternet.org/2013/09/05/part-2-concerns-about-personal-information-online/.

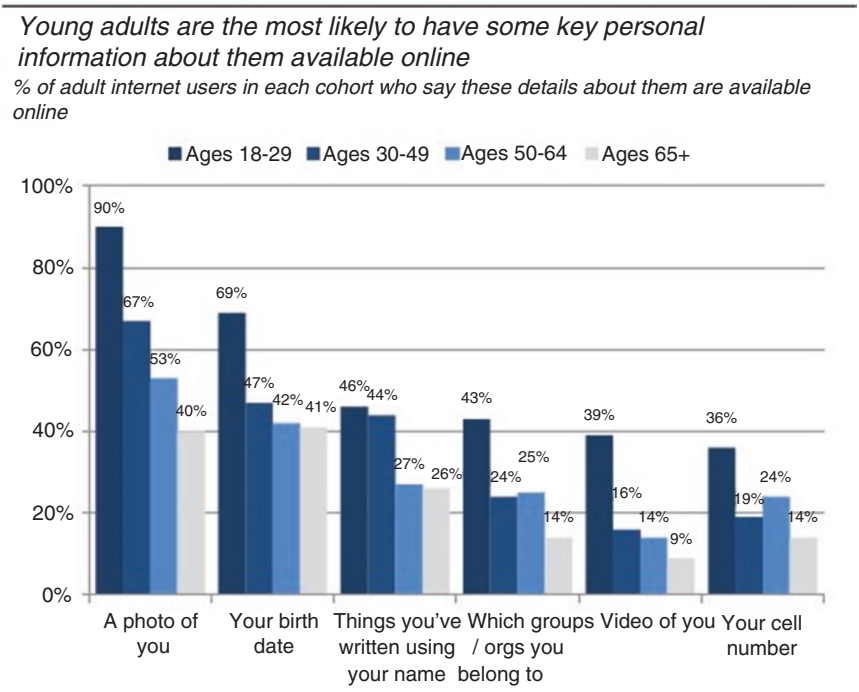

Fig. 6.1 The sharing of personal information online by differing age groups (Source: Pew Research Center.)

Governmental Surveillance Technology: How to Separate Positive Applications from Negative Uses

The use of surveillance, facial recognition, and monitoring tools is considered by some to be truly a threat to democratic values and individual freedom. A series of case studies about surveillance and control systems that are being used in urban areas around the world reveals a range of current practices.

In Russia, particularly in Moscow, a contract has now been awarded to install 130,000 cameras throughout the city. Further, many of these cameras have very high resolution—we are talking steerable, zoom-able telescopes mounted on swivel devices that can be remotely commanded. Currently there are only 1150 of these special cameras that are also connected to a two-way communications system that includes a database that contains images for ten million faces stored in the database's

memory. These special cameras link via a network to software developed by a company called NTechLab. This company has developed a program called "FindFace" that has bested software developed by Google capable of matching people to these database images that it can search through as they are walking on the street. This type of software surveillance software conjures up images straight out of *Blade Runner* as Harrison Ford talks to computerized tracking cameras that he uses to hunts down AWOL cyborgs.[12]

And the billion-dollar project is also being used to install Wi-Fi systems in classrooms, automate paid parking, and cover a wide range of medical- and health-related activities such as prescription ordering and fulfillment services, and automated medical appointment operations. This sophisticated system is now accessible by 16,000 city officials and especially 6000 law enforcement officials. The special cameras can be tightly focused in to even peek through windows. In Moscow it is increasingly possible for city officials and especially police to see who is doing what.

This billion-dollar investment into surveillance and oversight was purportedly started to address problems such as traffic congestion, monitoring of snow or trash pickup or the work of street sweepers, and aid in health, medicine and educational uses, but it is clearly now primarily a tool for anti-terrorism and policing. And this is not the most extreme use of surveillance systems around the world.[13]

In China the use of surveillance cameras is much more pervasive. A report that came from the BBC in early December 2017 indicated that China has now installed some 170 million surveillance cameras countrywide. Further, by 2020, another 400 million surveillance cameras are to be installed, to bring the total to nearly 600 million. As part of this report a BBC journalist agreed to have his face recorded and then walk about a city to see how long it would take for cameras to spot his location. It only took a few minutes for the surveillance sensors to pick up his location and monitor where he was going.[14]

Other reports by the Human Rights Watch indicated that the Chinese monitoring program is far more extensive. There is also a massive database that is actively assembling a tremendous amount of personal data on people in the minority region of Xinjiang by the police. This collected data includes DNA and blood samples, and iris scans. The data is apparently being assembled systematically as part of the free physical exams that are being offered to the public under the guise of a program called Physicals for All.[15]

The most concerning practice of all has been one that is at least 3 years old of creating for Chinese citizens what translated from Chinese as a social credit score. This

---

[12] Andrew Roth, "Letter from Moscow: Surveillance grows along with the city's tech", *Washington Post*, December 19, 2017, P. A5.

[13] Ibid.

[14] Christina Zhao, "China Used Its Vast CCTV Surveillance Network to Track Down Reporter in Just Seven Minutes" *Newsweek*, December 14, 2017 http://www.newsweek.com/tasked-trying-remain-undetected-long-possible-sudworth-filmed-himself-selfie-747843.

[15] "China: Minority Region Collects DNA from Millions" Human Rights Watch, Dec. 13, 2017. https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions.

score, which apparently is to be made a mandatory process for all Chinese citizens as of 2020, has been described as the collection of information on individuals based on such data as "financial transactions, shopping habits, social media, and interactions with friends, as well as other indicators such as traffic tickets and unpaid bills."

There is obviously concern that such a practice makes it difficult for any citizen to express a dissenting political view. Such a social credit score would create a sort of gaming mentality among the Chinese populace to reward support of the Chinese Communist Party by getting a high score. Instead of a penal process for dissidents with corporal punishment, this electronic monitoring system would actively encourage citizens to enthusiastically endorse the current policies and be rewarded for loyalty.[16]

This Chinese "Sharp Eyes" program is clearly aimed at providing by 2020 extensive surveillance of all citizens not only for purposes of criminal oversight but rather apparently for political control as well. The U. S. Federal Bureau of Investigation (FBI) has also moved to create in its Next Generation Identification System (NGIS) the ability to take video footage recovered from coverage of a crime scene and run it through a national data base of mug shots to seek a match. This system is reportedly only about 85% successful. It has been noted that the United States has some 62 million private and public video surveillance cameras in operation and thus on a per capita basis it has more surveillance cameras than does China.[17]

In the United Kingdom a Japanese surveillance system known as NeoFaceWatch has been used to identify people for arrest. In Chicago a thief was convicted in 2014 using facial recognition as the primary source of evidence. In short, we are entering into a new age of video surveillance in more and more countries around the world.[18]

The Pervasive Use of Biometrics in the Smart City

The use of what is called biometrics for identification has been around for some time. Fingerprint identification has been used for at least a half century. Today various biometric identification techniques are used, starting with fingerprints and iris scans. The linking of facial image biometrics to databases as noted in the previous section is becoming more and more prevalent and is now a key form of cellphone security identification. There are also systems linked to DNA, blood samples, and even body odor. The following examples of how biometrics are being used in society today include applications that many would find appropriate and useful, while others would see as intrusive to their own personal privacy.[19]

---

[16] "Here's Looking at You" *Washington Post*, Dec. 18, 2017 p A16.

[17] Simon Denyer, "The all-seeing 'Sharp Eyes' of China's security state" *Washington Post*, January 8, 2018, pp. A1 and A9.

[18] *Ibid.*

[19] Privacy Today: A Review of Current Issues, March 1, 2001 https://www.privacyrights.org/blog/privacy-today-review-current-issues.

What is perhaps shocking to some is that the uses cited below are not what are happening today but are from a report on privacy prepared in 2001:

- "Several airports in the United States and other countries have since installed facial recognition biometrics systems to identify individuals on law enforcement agencies' most-wanted lists."
- "Biometrics technologies are seen by the financial services industries as a way to deter fraud and identify fraudsters."
- "Many casinos now use facial recognition biometrics systems to identify known card-counters and cheaters and expel them from their facilities."
- "Various biometrics systems are being employed to provide secure access to computer systems, for example in health care institutions."
- "Many national governments, including the United States, use biometrics to speed border crossings and customs entry for frequent travelers."
- "Some states and counties use fingerprinting to prevent welfare fraud."

There have been reports that Disneyland utilizes facial recognition to connect guests' photos to their credit card information.[20] In discussions with a colleague at the World Bank I was told the only reason that we still have passports is because of the revenue stream. This is because biometric photo identification is now so pervasive the use of a passport is really passé as a reliable way to identify people at national borders. Passports may lie, but facial recognition biometrics according to Google and Apple I-phone technology is not fooled by fake beards or dyed hair or other disguises.

Business Uses of Rating and Surveillance Systems: Should There Be Controls?

Governments are thus using smart technologies not just to make cities more productive, control costs, combat crime and terrorism, and ensure greater public safety, but to engage in surveillance for other purposes—most typically to exert some form of political control. And the use of electronic technology for compiling information on individuals is no longer reserved just for use by governmental agencies and the police. The business community has embraced electronic intelligence as well.

The most obvious way that online information is captured by businesses is to engage in "cookie capture." This is the practice of noting who visits their site and catching the individual identifier for the computer as it logs on. Increasingly there are Internet users that have found ways to protect their privacy to mask their identity. Most companies now keep records of repeat customers and create incentives to keep

[20] "New Totalitarian Surveillance Technology, *The Guardian*, Aug. 15, 2012. http://www.guardian.co.uk/commentisfree/2012/aug/15/new-totalitarianism-surveillance-technology?newsfeed=true.

their customers loyal to them. The also provide incentives to customers to fill out questionnaires designed to find out if they are "loyal" customers or not.[21]

Current strategies involve such features as a "loyalty card" with a unique identifier number that provides discounts. This is common among restaurants, grocery and drug stores. Online retailers such as Amazon.com and Ali Baba offer "prime" customer incentives where customers pay an annual fee and then get features such as discounts and/or free shipping. These prime customers get special offers sent to their e-mail accounts based on either past purchases or, if they go shopping online, to look for various products or services. It is difficult to say when seeking to build customer loyalty reasonable efforts end and intrusion into one's personal lives begins. Customer "loyalty" dossiers can over time include information as to level of income, marital status, sexual preference, type of domicile, arrest record and other highly personal information. Credit information companies and even non-profit community aid or environmental organizations can create much more information than even relatives and close neighbors might know about an individual. Of course, once this information is compiled it might well be sold to others that might wish to either solicit a donation or sell a product to someone that fits their profile as a potential loyal customer.

Using Technology to Protect Privacy in an Internet-Driven World

As more and more people go online in smart cities in order to shop, work, bank, pay bills, their taxes and fines, chat, and play, they are clearly revealing themselves not only to employers, businesses, governmental agencies, and friends, but potentially to those that might wish to do them harm. The designers of smart cities can only do so much to defend the residents of their cities against cyber-attacks. Thus, the citizens that live in the world of tomorrow will need to do more to protect themselves.

The basic rule of thumb that all users of electronic media should observe is to purchase and keep up to date with privacy and cyber protection. This is, unfortunately, just part of the basic cost of living in the electronic world of today. This means that your computer, tablet and smart phone should be protected by an antivirus, a firewall, an identity theft protection service, and a virtual private network (VPN) service provider.

Sometimes this is all available as a package or by purchasing these services from only two digital privacy protection service providers. VPN providers often offer an antivirus and perhaps a firewall protection as an integrated package. These four types of digital privacy protection should provide reasonable levels of protection as

[21] Kay Ranade, "Customer Loyalty – What Is It? How Can You Measure and Manage It?" Loyalty Research Center, December 12, 2012 http://www.loyaltyresearch.com/insights/customer-loyalty-what-is-it-how-can-you-measure-and-manage-it/.

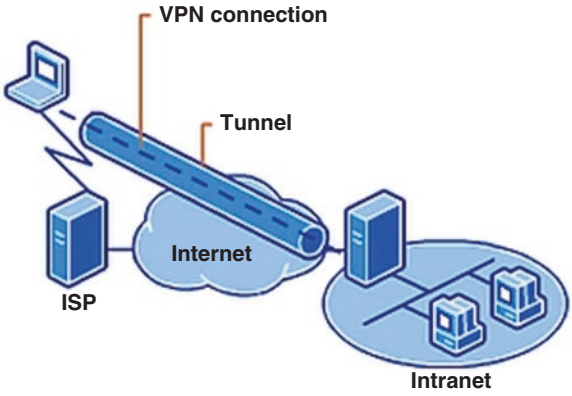

Fig. 6.2 This diagram shows how a VPN creates a "tunnel" to protect user privacy (Graphic courtesy of Microsoft.)

long as one restricts his or her access to websites that have URL addresses that begin: https. The "s" in the URL stands for security (Fig. 6.2).

Also make sure you sign up with a top-rated and known service providers. This caution is offered because there are fake VPN providers and other cyber-criminals that use unsuspecting Internet users as their prey by advertising protection when this is a phishing scam that is actually designed as a scheme to violate your privacy.[22]

Also, here is another warning. If you should sign up for an instant payment service on your credit cards, you need to keep them in a protected shielded container. This is because anyone with a scanner system that get in close quarters to your purse or billfold can also capture your credit card information and be off on a shopping spree. The cyber-security chapters later in this book will explain protective efforts in greater depth, but the message here is that there are a number of protective steps that should be taken regardless of what type of computer or smart phone device you use. Macs might be safer, but all computers are potentially at risk from cyber-criminals.

Blockchain Technology and Concealed Identities

Some believe that the next step beyond purchase of cyber-defense software is to enter the world of crypto-currency and "blockchain" protective technology. This objective would presumably be to protect your finances and to shield your assets from prying eyes. The prime application for block chain systems and operations that involve establishing a confidential blockchain ledger is for crypto-currency exchanges such as Bitcoin, Etherium, Ripple, Bitcoin Cash, Litecoin, Cardano, IOTA, Dash, NEM and Bitcoin Gold. These crypto-currencies represent the current top ten capitalized electronically traded currencies. The current market capitalization Bitcoin and its nine

[22] Lee Mathews, "Fake VPNs Are Trying to Cash In On Your Online Privacy Fears" *Forbes CyberSecurity*, April 5, 2017. https://www.forbes.com/sites/leemathews/2017/04/05/fake-vpns-are-trying-to-cash-in-on-your-online-privacy-fears/#f329bdc7c1cd.

other "wannabes" is around $550 billion in "assets" as listed on the currently listed market exchange for cryptocurrencies as of the end of January 2018.[23]

All of these currencies depend on block chain-based exchanges to carry out purchases with participating companies. But there are potentially more applications that might be made of block chain ledgers in a wide range of other areas to provide greater security and add to personal privacy. Advocates have said: "While the most popular use of block chain technology is bitcoin and other crypto-currencies, the wider picture is that distributed ledger technology is decentralizing, democratizing and disrupting sectors like finance, property tech, education, governance, and more."[24]

In short some are arguing that the security that comes from the "seed phrase" of 12 words randomly selected from the dictionary and then twice converted into a series of 64 numbers and characters are protected against ever being decoded. This super-secure cryptocoding process could represent a whole new approach to creating cybersecurity, especially where there is an exchange of goods, value, or information, but also as defense against distributed denial of service (DDoS).[25]

The key to the so-called distributed ledger technology is what is called a smart contract. A smart contract is defined as "automatically executing pieces of code that can carry value, data, or other such condition-based execution."[26] This push for privacy, borderless and clandestine currency, and anonymous communications that has produced the deep web, the dark web and the growth of "distributed networks" is in some ways a response to governmental regulatory overreach on one hand and terrorists and criminals on the other. It is a basic dichotomy in modern electronic society. Many people do not know whether to hail people like Edward Snowden who revealed National Security Agency intrusions into the privacy of citizen's homes or to support his indictment for revealing state secrets. For many people it might even be both.

The moral of this discussion is that there is ultimately no single technological fix to privacy and the protection of democracy values. Any real solution will likely involve new regulations, new legal provisions and court decisions, and recognition that a free press and free speech in a society is the only way to preserve democracy. People rightly are concerned about terrorism, but far more people die due to heart attacks, cancer, automobile accidents, and other activities—including opioid addiction and murder—at least in the United States. These are problems that medical research, technology and even legal reforms can more easily address. Privacy, democratic values and prevention of terrorism represent special problems that require a wise and balance approach to legal reform that considers a moderated approach to the use of technology.

---

[23] Cryptocurrency Market Capitalizations, December 21, 2017 https://coinmarketcap.com/.

[24] Ryan Kh, "Cybersecurity Is a Mess; Can Blockchains Fix It? Catalyst for Business, December 21, 2017. https://www.infosecurity-magazine.com/next-gen-infosec/cybersecurity-mess-blockchains-fix/.

[25] Steven Johnson, "Crypto-currencies aren't just about making a fortune", *New York Times Sunday Magazine*, Jan. 21, 2018, pp. 36–40.

[26] *Ibid.*

The over-reach of governmental or commercial practices that invades people's privacy, limits their free speech, and muzzles the free press will ultimately be self-defeating. Again, it must be said the goal of the smart city is not technology for technology sake. The objectives are to be effective and cost-efficient, but too much monitoring, too many controls, and too extreme levels of automation can become counterproductive. The goals for a safe city at the highest level must be to make its citizenry safer, more prosperous, and yes, even happy. The misuse of technology can subjugate the rights of citizens and thus ultimately suppress freedom, liberty and democratic controls. The maintenance of that balance is thus one of the most critical challenges in designing, operating and improving life in the smart city.

Possible Constitutional, Legal and Regulatory Reforms

There is no single formula that indicates what types of constitutional, legal or regulatory reforms will keep on track the new technology that enables a smart city to operate efficiently and effectively. The top guideline is to preserve to the highest degree practical the constitutional rights of citizens to exercise free speech, to assemble and protest governmental actions, to vote, to have a free press that is not subservient to the government, and to preserve a legal system that conducts fair trials, and observes fair judicial, legal, and criminal prosecution proceedings that are consistent with laws of the land enacted by a legislative body that is duly elected. This is usually summed up by saying that a country observes "the rule of law."

It is getting ever more difficult to control technology now that it plays such a large role in governmental, police, military and business operations. Indeed, it permeates our lives almost like the air we breathe. The dilemma about choosing between "good technology" and "bad technology" and creating the right standards, regulations, laws and constitutional provisions is downright tough. Let's wrestle with some difficult decisions, such as how to allow the "good" but then also prohibit the "bad" technical applications. Just how hard this is will be revealed in a few case studies. There are clearly instances where one use of a technology will generally seem to be good, but yet another application of that same technology will seem bad—or at least strongly undesirable.

Case Study #1: Use of Satellites, High Altitude Platform Systems (HAPS), UAVs and Drones for Observation and Communications

Remote sensing satellites and other types of platforms flying in space or in commercial air space are increasingly adept at using sensors of various types (radar, infrared, hyper-spectral cameras, high definition telescopes, etc.) to provide more

and more precise information about conditions in the atmosphere and on the ground. It is now possible for satellites to monitor quite accurately the buildup of carbon dioxide, methane and other greenhouse gases. It would be possible to create quite accurate global monitoring systems using a worldwide network of satellite-based monitors.[27] It is also possible for broadband wireless to be sent to and from drones and HAPS to provide video surveillance, television broadcasts, and support fourth and fifth generation wireless services as well as navigation services.[28] Such applications could make train, bus, truck and car transportation systems safer through improved traffic control. It could be used by the military for defensive operations and to support soldiers in the field. Business retailers could count cars in parking lots to monitor customer buying patterns. City planners could monitor patterns of growth in urban regions, and maps could be updated in near real time. Information on pandemic outbreaks, the spread of petroleum from oil spills or the paths of drug smugglers could be closely tracked and charted with accuracy. Most would likely find these applications positive tools that would aid the operation of the smart city.

However, what if these same tools were to be used in aid of a totalitarian regime that installed tracking devices on enemies of the state and political opponents to suppress citizen protest and impose strict control on resident behavior with armed drone policing agents. The technologies needed to accomplish these two types of tasks are disturbingly similar. The protection is not in outlawing the technology but in supporting basic constitutional rights to ensure the rule of law and democratic processes. As frightening as terrorism might seem, the use of Big Brother-like systems must be banned, and constitutional rights of democracy and personal liberties ensured.

Case Study #2: Use of Wi-Fi Hot Spots in Central Locations of a Smart City

Wi-Fi and Wi-Max broadband services that are provided pervasively throughout a community are able to provide convenience to the public at large and make city-based services more extensively available at essentially little or no cost. One can access bus schedules, check out an e-book from the library, report a pothole in the street or even pay taxes or a fine. Urban-owned and operated Wi-Fi systems are able to extend city services to the community faster, better and at lower cost.

Yet the Wi-Fi network could also be linked to surveillance cameras installed across the community and especially in commercial areas and centers of government. This would not only allow the constant monitoring of people but also the instant transfer of images via the Wi-Fi centers into a database. It could also enable the searching of crowds for particular targeted individuals with their facial characteristics now captured. This in turn could be used to link up images of people to their credit card

[27] Tom Risen, "CO_2 Watchdogs" *Aerospace America*, January 2017, pp. 22–28.

[28] Brian Fung, "Wireless for drones, trains and automobiles" *Washington Post*, May 7, 2017, pp. G1 and G4.

information and driver's licenses in an effort to create an even more systematic database and intrusive catalog of "citizen profiles." As noted earlier in this chapter such a set-up is not a theoretical scenario. A similar set up is now operational in Moscow, and this includes a database with ten million people now included.

Again, cameras and Wi-Fi hotspots across a smart city can add value and extend the scope and range of services available to residents and businesses, but such a network can be reversed from being optimized to offer services to become a tracking and monitoring system for policing or political monitoring of opponents. Unless there are strong controls and legal constraints on such interactive systems then abuses can abound. Again, the key is the rule of law rather than defining the limits of technical systems, justice and democratic controls.

Case Study #3: The Internet of Things for Updating of Software on Computers and Cars

In the next few years the increase in Internet of Things-equipped devices will mushroom. Virtually every commercial consumer product, from dishwashers, electric skillets, toasters, and baby monitors to cars, trucks, and tractors, will be equipped with literally billions of IoT units. The projections are that this will lead to a 15-fold increase in machine-to-machine (M2M) data transmission and a 50-fold increase in stored data between 2016 and 2020.[29] This transformation of the "electronically aware" world we live in will allow software updates to make products last longer and to offer a broader range of services. Thus, updates to IoT-enabled devices can make phones, tablets and computers more secure, battery systems and car fuel injectors more efficient and help engines last longer. But if the access codes fall into the wrong hands, cars and even trucks and buses can be sent commands to make them crash with potentially fatal results. Actual recorded instances of abuses that have already occurred include hackers being able to look through baby monitors and burglars being able to use video monitors and alarm systems to see when no one is home so they can engage in robberies. An enterprising hacker was able to hack into a smart aquarium at a casino and from there link into the casino's database to steal stored credit card information of customers. The question that arises here is whether the purchasers of IoT-enabled devices for automobiles and appliances should have the right to turn off IoT devices or alter access codes to protect their privacy and prevent potential attack via smart devices in their home or vehicle. In some instances, a smart house could mean an abode that is under surveillance by a criminal hacker or in some cases even by governmental monitors.

[29] White Paper on IoT for Defense, Wind River, Dec, 2017 http://www.windriver.com/whitepapers/iot-for-defense/wind-river_%20IoT-in-Defense_white-paper.pdf.

Case Study #4: Cloud-Based Computing Services for City Payroll and Tax Payments

There is an ever growing use of cloud-based systems for low-cost information storage, for super computing power, for special processing software, and more. This increasing use of the cloud is for businesses—large and small—governments and organizations, and even for individuals who have special processing requirements related to security systems, large amounts of data, etc. The assumption made by most people is that the cloud provides low-cost data storage and secure and sophisticated processing capabilities. But there are vulnerabilities here as well. There is always the concern that there could be an inside breach of security from the staff of cloud operators. There is also the concern that there might be crossover breaches between one database and another.

This is a privacy challenge for cities that store their vital tax and financial records within a cloud service provider's database. In this case businesses and organizations as well as individuals might find their banking records or other confidential information hacked by cyber-criminals or even techno-terrorists. Indeed, in the case of very large cities vital information stored by cloud service providers might expose types of information such as code accesses to valves on water supplies or sewage processing plants or even controls to water cooling systems for nuclear reactors. Of course, urban databases are also potentially vulnerable to attack, but in the case of large volume cloud service providers such as Amazon Web Service, Microsoft Azure, IBM Cloud and a Google cloud platform, these huge global marketplace database systems become extremely attractive targets of attack.[30] (See Fig. 6.3.)

And it is not only the cloud service providers but also outside IT service providers that could also be attacked to obtain vital and carefully protected urban community databases. The top ten of these type organizations for 2017 are: Accenture, Cognizant, IBM, Tata Consultancy Services, Wipro, HCL, Cap Gemini, CSC, Infosys, and Atos.[31]

The over centralization of information just for cloud service providers has thus become a concern with regard not only in terms of possible hacker attack or insider breach, but also in the context of too much information being amassed in a single source location. As a consequence of the Nazis taking over national databases during World War II, the governments of Norway and Sweden rigged their national databases with explosives to destroy on command these systems as a protection against arbitrary and unauthorized future access. Many fear that the creation of too much sensitive information at a single source could potentially become a threat to democratic processes. This has led to such activities as the creation of crypto-currency,

[30] Cynthia Harvey "Public Cloud Computing Providers" *Datamation*, April 26, 2017 https://www.datamation.com/cloud-computing/public-cloud-providers.html.

[31] Setphanie Overby "Outsourcing the top ten IT service providers" Dec. 4, 2017 Everest Group, CIO https://www.cio.com/article/3030989/outsourcing/the-top-10-it-outsourcing-service-providers-of-the-year.html.

Fig. 6.3 This cloud service provider data storage facility is capable of storage of exabytes of data (Illustration courtesy of George Washington University.)

off-shore "fat-pipe" encrypted data havens (such as Sealand in the North Sea) and most recently even an encrypted smallsat, the Asgardia 1, that was launched as an orbital data haven.[32]

Case Study #5: Artificial Intelligent Heuristic Systems to Mitigate Traffic Jams and Moderate Energy Usage

The scientist, futurist guru and science fiction writer Arthur C. Clarke stated that the most important invention of modern technology was artificial intelligence. Entrepreneur Elon Musk has urged extreme caution in the enabling of machinery, especially war-fighting instruments, with too much artificial intelligence. We certainly have been exposed to dystopian examples of how artificial intelligence could go awry. The stories of out of control AI computer villians range from the computer HAL in *2001: A Space Odyssey* to the Skynet computer in *Terminator 3* to "VIKI" in the movie *I Robot*. One does not have to jump to scenarios of run amok robots and hostile computer logic systems to anticipate how AI systems might possibly bring harm to a smart city in the future.

Increasingly smart programs, expert systems, heuristic algorithm, and if-then logic systems are assuming increasing controls of driverless cars and automated parking operations, building elevator systems, transit systems, water purification and sewage treatment plants, and more. The reliability of these systems can be quite

[32] "Welcome to Sealand, Now Bugger Off" Wired, July 1, 2000 https://www.wired.com/2000/07/haven-2/.

high. Most such AI systems have indeed proven to be more accurate and reliable than human operators. The December train derailment in the State of Washington in the United States presumably would have been prevented if a positive train control (PTC) system had been activated that would have automatically slowed the train from 80 miles per hour to the posted 30 miles per hour speed limit for this curved part of the track that also spanned an interstate highway. It is now widely assumed that a distracted railroad engineer may well have contributed to the speeding train accident.[33]

The problem is that if a hacker is able to access the AI programming and then corrupt it or substitute an alternative program or gain access to communications channels that can alter programmed instructions, then the potential exists for terrorist attacks by sabotaging speeding trains, nuclear power plant cooling control systems, water and sewage treatment plants, or traffic signal systems.

Further if these attacks on AI systems could be designed in the form of computer viruses that could mounted against hundreds or even thousands of cities at a time, such as we saw with the WannaCry attack that occurred in May 2017, the seriousness of the threat becomes clear. Such an attack, if it could disable health care and educational systems, water treatment plants, traffic control systems, energy networks and nuclear power plant cooling systems, would become the equivalent of an assault by a weapon of mass destruction.[34]

This strongly suggests that emergency overrides, fault detection systems, and limits to alterations of automated AI programing are needed with confirmation codes to authenticate program changes. By way of example, the Intelsat Global Satellite Network has a requirement that commands to its orbiting satellites must be confirmed with authentication codes from another tracking, telemetry and command station. This is a basic precaution to avoid spurious commands that might come from hackers seeking to attack a communications satellite safe operation. In addition to this type of technical precaution, it is also important to move to legislative action to make any such sabotage to any key urban infrastructure a very serious felony with extremely severe penalties, including life imprisonment in the case of loss of life from such attacks.

Finally, there is an even more fundamental point to consider about the future consequences of AI on global society and the smart city. This is the economic impact of AI systems replacing at an ever increasing clip many types of service jobs. As Kai-Fu Lee, chairman and CEO of Sinovation Ventures and president of the Artificial Institute, has stated: "These [AI] tools can outperform human beings at a given task. This kind of AI is spreading to thousands of domains…and as it does, it will eliminate thousands of jobs. Bank tellers, customer service representatives,

[33] Terrence Cullen and Leonard Greene, "At least three killed after Amtrak train derails in Washington" Daily News, Dec. 19, 2017 http://www.nydailynews.com/news/national/high-speed-amtrak-train-derails-washington-state-article-1.3707034.

[34] Craig Timberg, Griff Witte and Ellen Nakashima, "Malware Attack Hits Global Networks" Washington Post, May 14, 2017. pp. A.1 and A11.

telemarketers, stock and bond traders, even paralegals and radiologists will gradually be replaced by such software."[35]

Rising urban populations and a shrinking number of service jobs fueled by AI technology may be the greatest urban challenge of the next few decades. In this area there are no clearly available technological or legal remedies in sight. Some further believe that the key cities that are powering the growth of high-tech industries, autonomous robotics, and AI-controlled systems are becoming "untethered" from the rest of the world's agricultural regions, which are rust-belt zones of unemployment, and that this is accelerating the gap between the haves and the have-nots in the global economy.[36]

Case Study #6: Systematic Urban Polling of the Citizenry

Another recent innovation in smart city technology is the ability to rapidly poll the citizenry with regard to features that might be implemented. This type of capability, if it could provide citizen input from many thousands of citizens about urban services on an instantaneous basis across a wide spectrum of users, would seem to be a very good thing. The concern would be if such an instant public opinion poll were somehow rigged. Then this could stand such a process on its head and could become a tool for manipulating public opinion and actually would become an anti-democratic weapon in the hand of a totalitarian ruler. Actually, such an electronic system to poll citizenry on issues is now in effect in Moscow, and it is called "Active Citizen."[37]

The design of this electronic polling system purportedly includes a block chain ledger architecture that insures that input is insulated from being manipulated. This results in a secure list of records that keeps track of verifiable transactions. As such it is claimed that this type of system is guaranteed against abuse. Today this system can be used to poll citizens on what to name a Moscow metro stop, select the best ways to celebrate a holiday, or even vote on the multi-billion dollar renovation of the city to modernize it from top to bottom. There are skeptics, however, that believe that on important issues, this elaborate system could be rigged to produce the outcome that political bosses have already decided are the "right" outcome.[38]

---

[35] Kai-Fu Lee, "The Real Threat of Artificial Intelligence" Washington Post, New York Times, June 25, 2017.

[36] Emily Badger, "The Megacity, Untethered", *The New York Times,* Sunday Business Section, Dec. 24, 2017. pp. 1 and 6.

[37] Andrew Roth, "Surveillance grows along with city's tech", Washington Post, December 19, 2017, p. A5.

[38] *Ibid.*

Case Study #7: Russian Trolls Spreading False Information in Seeking to Sway Voter Opinion in Favor of Donald Trump and Against Hillary Clinton in the 2016 U. S. Presidential Election

The idea that one sovereign nation might intervene in the election of another to influence an election is not a new concept. In Europe, going back centuries, marriages were arranged between royalty involving Germany, France, England, Spain, Italy and even Russia just for that very purpose. The new ability to use the Internet trolling and robot messaging that fakes the opinions of real people represents a new type of technological assault on free elections. And the U. S. presidential elections of 2016 represent only one example. The process continues around the world even today. Iran is engaging in such activities to destabilize democratic processes in the Middle East. China has been accused of engaging in this practice in Taiwan (via a "fake new" site known as LINE), and Russia has been explicitly accused of continuing this practice without pause even after the 2016 elections. Explicitly Russian trolls have been accused of using social media to attack the FBI investigations related to media misrepresentation in the 2016 U. S. elections. A site #boycottheurig, attributed to Russian trolls, attacked in October 2017 a U. S. company for withdrawing advertising from Sean Hannity's Fox News Show after Hannity defended positions that the Heurig Company found objectionable.[39]

The use of the Internet, texting, and the encouraging of re-tweeting of "fake news" messages to influence public opinion is a dangerous new trend that is hard to control within a democratic society where free speech is a core value. The abuses created by robotic trolls operated by foreign governments in a campaign against other governments are now seen as an increasing threat that is difficult for democracies to control without stifling true free speech. A recent extensive report from the *Washington Post* on this subject singled out Russian efforts in this regard as follows: "When President Putin came to power, Russia began searching for ways to make up for its diminished military. Officials seized on influence campaigns and cyberwarfare as equalizers. Both were cheap, easy to deploy and hard for an open and networked society such as the United States to defend."[40]

Some are now seeking to hold social media providers such as Facebook, Twitter, Snapchat, etc., accountable as publishers rather than just platforms in a world in which millennials get more "news" from social media than conventional news outlets. Twitter, in response to criticisms, has now begun a process whereby it is suspending violators, users that are systematically providing racist, hateful, violent, abusive or 'fake news' content. Thus, under this policy, Twitter has banned Alt-right Britain First among others and is working with experts to identify others that should

[39] Michael Morell and Mike Rogers, "Russian Cyber-attacks Never Stopped" *Washington Post*, December 26, 2017, p. A17.

[40] Adam Entous, Ellen Nakashima, and Greg Jaffe, "Kremlin's trolls beset Web as U.S. dithered" *Washington Post*, December 26, 2017, pp. A1 and A6-A7.

be suspended. Twitter has indicated that it will create an appeals process to review their suspension. It will be easier for social media officials to enforce such suspension processes than for governments to engage in censorship.[41] One of the promising areas of current research are AI-based programs that can be used to detect bot operations on social media and the ability to systematically remove them by social media operators.[42]

Conclusions

The world of technology and AI-controlled management systems that is being embraced by the urban planners of tomorrow's smart cities is complicated to say the least. The latest computer processors, software and artificial intelligence have the potential to work truly amazing miracles of efficiency and provide substantial labor reductions and cost savings. These technologies and automation of key processes can combine with new forms of urban infrastructure to expand city services. Modernized systems can offer safer streets, more energy efficient networks, less polluted water and air, and what most would generally consider to be more livable communities.

The pursuit of such efficiencies, however, can tend to lead urban officials, planners and technology to overlook potential downsides to some new and highly automated urban systems. Some of the key questions that need to be assessed before embracing new technology are:

- Will automated systems accelerate either unemployment or underemployment, and what are the longer term implications in terms of city prosperity, tax base and other civic concerns such as crime and vagrancy?
- Are new automated or modernized systems adequately protected against cyber-attacks by terrorists and hackers, and are they engineered so that any such attacks can be minimized on their size, scale, impact, and time of recovery? This includes key questions about the protections provided by a vibrant and effective human-machine interface.
- Are there endemic dangers related to automated technological systems and/or public survey networks that might thwart basic democratic values and protections? Such concerns might be related to political liberties, corruption of decision-making processes on the part of urban leadership, freedom of expression, voting rights, referendums, fair judicial processes and legal reforms or appeals.
- In the world of smart cities with the potential for over exposure to social media, especially by younger people, are there true social, educational, and behavior

[41] "Twitter's Haphazard Purge," *Washington Post,* December 26, 2017, p. A16.

[42] Denis Stukal, Sergey Sanovich, Richard Bonneau, and Joshua A. Tucker, Detecting Bots on Russian Political Twitter, *Research Briefings*, December 2017. http://online.liebertpub.com/doi/full/10.1089/big.2017.0038.

problems and issues that need to be addressed? These include what Sean Parker, the first president of Facebook, has called the dangers of "a social validation feedback loop."[43]

- Are there hidden dangers, longer term maintenance, repair, and upgrade costs that could balloon over time, new dependence on outside consultants that leave the city vulnerable to infiltration or attack, or other unsuspected concerns or costs?

These are only some of the bigger picture concerns that urban leadership must consider before approving modernization or new smart city systems. There are, as can be seen in the case studies presented in this chapter, hidden concerns and implications that should be carefully evaluated.

The fundamental questions are, will this change make the community a better place to live, maybe not tomorrow or next week but in future? Do short term economies or labor reductions really offer sufficient benefits for the community in terms of its longer term goals? Are there key protections related to safety, public security, guarantees against cyber-attacks or breakdown of automated systems that need to be considered and implemented before proceeding? Is it best to have a trial test of performance, reliability, or systems that protect political liberties and freedoms before proceeding to full-scale implementation?

[43] Op cit Z. Tufekci.

Chapter 7
A 21st Century Smart City and Mobility

Today's smart cities depend on broadband systems for every aspect of their operations. Municipal systems for transportation, energy, health and education, water, sewage, and other vital services heavily depend on broadband networks. In addition, virtually all forms of businesses would be severely compromised if they lost their broadband mobility networks. On top of everything else security and video surveillance systems that protect cities and aid first responders are dependent on broadband systems. Especially challenging is the ability of broadband wireless systems to keep up with demand because of the frequency shortages due to rapidly escalating public and professional demand for expanded services.

A 2013 White Paper, prepared by the U. S. Federal Communications Commission, sought to project the growth in demand for broadband wireless services. This White Paper also sought to compare projected U. S. growth rates to trends in other countries around the world as well as to compare spectrum assigned to wireless communications in both licensed and unlicensed radio frequency bands. The results shown in this official document were heavily based on a detailed study undertaken by the Cisco Corporation. The shocking results from these studies and forecasting profiles of broadband wireless mobile growth were disturbing. It was not so much that the forecasts predicted soaring demand for massive new wireless broadband throughput and consequent huge spectrum demand that would escalate 18 times in the 5-year period between 2011 and 2016. No, the shock came from the responses saying that Cisco had not projected demand at high enough levels. Indeed, most people believed that the growth estimates were far too low[1].

The FCC has stated their forecast of surging growth in their White Paper in this manner:

[1] Cisco White Paper, Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2011-2016, Executive Summary, February 14, 2012, available at http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html (Last visited Jan. 10, 2017).

© Springer International Publishing AG, part of Springer Nature 2019

J. N. Pelton, I. B. Singh, *Smart Cities of Today and Tomorrow*,
https://doi.org/10.1007/978-3-319-95822-4_7

The mobile wireless landscape is undergoing a transformation, as mobile broadband networks are emerging not only as the foundation for communications services in the twenty-first century, but also as the infrastructure supporting economic growth and innovation in wide-ranging, consumer-focused areas such as health care, public safety, education, and social welfare. Ensuring that sufficient spectrum is available to satisfy the growing demand for mobile broadband services is a global challenge: global mobile data traffic is anticipated to grow eighteen-fold between 2011 and 2016.[2]

In fact, growth rates in usage and consumer demand were generally in line with the predicted result, not only in the United States but also in Europe and other countries, with high penetration of smart phones. The industrialized countries have already allocated on the order of 600–800 MHz in licensed and unlicensed spectra to mobile broadband wireless services. The reallocated bandwidth for such service has largely come from over the air commercial television and radio, dispatch radio services, educational television, satellite communications, microwave relay services, and even some military communications services. In some cases, it has not been a full reallocation of spectrum but reassigning bandwidth dedicated to other purposes being moved to a shared usage basis. And the surge in growth has in no way abated. Current estimates suggest that demand for 5G broadband mobile services might increase as much as 40 times in the next decade through 2030.

Coping with Future Needs

The key question is where huge new lumps of spectrum bands needed to accommodate this continuing growth come from in the future. How do we cope with the burgeoning demand that continues to surge forward in the years ahead as the needs of the smart city and broadband wireless become inextricably linked? Currently the demand for broadband mobile services continues to grow apace. The relatively near term introduction of the fifth generation (5G) broadband mobile service in the United States, Europe, and around the world will only accelerate the demand for mobile services and spectrum. These ever more intensive efforts to carve out new allocations for broadband mobile cellular services in particular has become a zero sum game played against all sorts of other telecommunications and networking service providers such as satellite companies, emergency dispatchers and first responders, etc.

On one hand the continued reallocation of spectrum is popular with politicians in that the government in proceeding to auction off this new spectrum for broadband mobile cellular service now known as “5G Long Term Evolution (LTE) service” represents a major new source of public revenues. Further public constituents see benefit from having this broadband spectrum even if the most popular use is to see television sports, news and entertainment on their smart phones. At the next World Radio Conference (WRC) advocates for broadband mobile services will likely push

[2] FCC White Paper, The Mobile Broadband Spectrum Challenge: International Comparisons, Feb. 26, 2013. https://apps.fcc.gov/edocs_public/attachmatch/DOC-318485A1.pdf.

for most of the millimeter wave spectrum to be allocated to these type uses. Others will resist this temptation and argue to keep some spectrum for new low-Earth orbit satellite communications networks, high altitude platform systems and other applications. The bottom line is that new advanced coding techniques that allow both new efficiencies and sharing between terrestrial mobile and satellite services will be keys to meeting all global needs. The smart city applications for autonomous transportation systems, Internet of Things (IoTs) security and efficiency applications will be dependent on finding enough spectrum to meet these accelerating needs and uses.

On the other hand, some of the frequencies under attack for reallocation are now used by first responders such as police, firefighters, EMT trauma technicians, military personnel and satellite service providers. These service providers are all fulfilling urgent societal needs, but those needs vary around the world. Clearly technological breakthroughs in terms of more efficient encoding and multiplexing, and ability to transition to higher spectral bands such as from microwave to millimeter waveguides are foreseen as providing part of the answer.

Also, over the air television and radio broadcasters are now able to use digital technology and encoding to provide their services much more efficiently, and thus also free up new spectrum. The laws of physics that control the total amount of radio frequency spectrum available in the universe are not easily tampered with to create totally new frequencies to use. An 18-fold expansion of demand and new allocations to accommodate this growth might happen once, but it such runaway growth cannot continue.

This is a problem for the International Telecommunication Union (ITU) and national frequency control agencies. For this book, there is an issue that transcends the problem of how mobile telecommunications and networking applications get more spectra to accommodate accelerating growth. This issue is what does this more intensive use of radio frequencies for more and wireless applications mean for personal, governmental, and military security? The advent of more and public websites and more services that are offered via HTTP sites rather than HTTPS, means more opportunity for cyber-criminals to exploit vulnerabilities. The ever more rapid growth of new "apps" that can be loaded onto smart phones is the yawning problem that most consumers are actually frequently unaware of and not well equipped to defend against successfully.

Cybersecurity for Broadband Wireless

There are today a number of "toolkits" that can be purchased to allow programmers to develop new apps to load onto smart phones for every conceivable purpose. This may be to purchase a hamburger, subscribe to a newspaper, play a video game, engage in electronic banking, access your medical records, file a tax return, or log into a porno site. The purpose of the particular application is not important. The fact is that many of these applications are means for a cyber-criminal to hack your phone to get vital information about you, your bank accounts, your social security number, your medical records, and information about your family and friends. The kits that

are designed for accessing android phones allow more opportunity for hackers (more appropriately called "crackers") to access your smart phones, but Apple smart phones are not entirely immune from attack.

Several rules of thumb can be used to provide at least some level of increased protection. The following protective practices are highly recommended:

- *Do not load up your smart phone with scores of applications.* Instead choose wisely the best and most needed applications that have been developed by respected companies and represent applications you use often as a part of your daily life. Avoid promotional applications such as free video games or free video greeting cards. These are often not only "cookie catchers" that are sold to web-based spammers, but sometimes much worse, such as to attack your smart phone by loading malware on it. Most of these "bad apps" may be simply trying to get your e-mail to sell to marketers, but the more apps loaded onto your smart phone, the more vulnerable you are to an attack by seriously dangerous malware. The bottom line is that the more apps you have loaded onto your smart phone the greater the risk not only to your privacy but to your bank account and your financial and personal well-being.[3]
- *Do research on the various apps that you choose to implement to find out if they are vulnerable and to determine if they are particularly prone to being hacked.* There are many apps that have been developed from toolkits that are notable for having back door access that make it possible for cyber-criminals to access all of the information on your cell phone. This is, of course, likewise true for your home computer, I-Pad or any other electronic device on which you store information. The key is to purchase applications directly through Apple, Google or other similar vendors, which do not use macros in their apps software that are potentially hackable.
- *Be particularly cautious about using RFID enabled credit cards for instant payment using near field communications (NFC) readers at commercial vendors.* This may seem quite convenient, but there are several vulnerabilities with this type card. There are portable RFID reader kits that can be used by cyber-criminals at close range to read you card. Unless you have a protective casing for your credit card or cards that can act as a "Faraday cage," you are vulnerable to having your card electronically stolen and counterfeited. Many of the companies that use near field communications readers have not adequately protected against attacks on their databases or cyber-criminals setting up shop with their own reader in proximity to the store's reader.[4]

These are only the most vital precautions. The chart below as developed by Sid Kirchheimer in his quite useful book provides a ten point check list of precautions

[3] Joseph N. Pelton and Indu Singh, *Digital Defense: A Cyber Security Primer* (2015) Springer Press, NY. pp. 89-91.

[4] Thomas S. Heydt-Benjamin, Daniel V. Bailey, Kevin Fu1, Ari Juels and TomO'Hare, Vulnerabilities in First-Generation RFID-enabled Credit Cards – SPQR https://spqr.eecs.umich.edu/papers/RFID-CC-LNCS.pdf.

that should be taken to protect against your smart phone from being hacked and vital information from being stolen from you to steal money from your bank account or perhaps to even blackmail you over information you would not want publicly disclosed. The first step is to behave, do not have affairs or embezzle from your firm (Table 7.1).

For further advice to protect yourself from hackers accessing or hacking your smart phone see Sid Kirchheimer, *Scam-Proof Your Life: 377 Smart Ways to Protect You & Your Family from Ripoffs, Bogus Deals & Other Consumer Headaches* (2007) Sterling Press, New York.

Table 7.1 Recommended steps to secure your smart phone

Ten Recommended Ways to Protect Your Smart Phone and Electronic Devices
1. Always activate encryption on your smart phone. Choose a vendor that provides it and one that is highly rated. Always be sensitive to protecting your privacy.
2. If your Internet service provider or smart phone provider recommends you use particular security software, then proceed immediately to have it installed. There are several free products that can very usefully be installed on your phone in order to help protect it. These can include AVAST, Panda, Lookout Mobile Security, AVG, and others. These can also help with phone location if stolen. (See no. 7 below.)
3. Be careful about installing any new apps on your smart phone, I-Pad, laptop or desktop computer. Don't go to suspicious or X-rated websites. These are the primary ways by which cyber-criminals can access your smart phone. Thus, only buy apps from websites such as Google, Apple, etc. Also, never save your password on any apps. This is a critical cybersecurity rule of thumb.
4. Be cautious about using publicly available Wi-Fi systems, and avoid banking or undertaking financial or stock market transactions on such sites. It is always better to use your home computer with a secure hardwire connection to your Internet service provider.
5. Don't leave any access connections to the Internet open and turn off your electronic devices when not in use. If you have a wireless chip in your cell phone, tablet, laptop or any electronic device others can access it with the proper air interface standard.
6. Clear your browser history on all electronic devices. This can be used by cyber-criminals in a variety of ways, and this is yet another way to preserve your privacy.
7. Activate an application such as "Where's My Droid" or the I-Phone software to help you to always locate your phone and to help police find your phone if stolen. (See no. 2 above. Security software can also provide other protections as well.)
8. Back up your most important data on your desktop computer, smart phones and I-Pads either on a hard drive, high capacity flash drive or via a service that does it automatically at short intervals. These services can also provide protective services to make you anonymous on the web.
9. If your phone is stolen and not recovered, you can contact your carrier to remove sensitive data that was stored on it.
10. Lock your phone with at least a PIN number, but it is best to have an even more secure system such as facial recognition or where you are required to draw a design together with facial recognition.

Sid Kirchheimer. *Scam-Proof Your Life: 377 Smart Ways to Protect You & Your Family from Ripoffs, Bogus Deals & Other Consumer Headaches* (2007) Sterling Press, New York. Also see Chapter 5 of Joseph N. Pelton and Indu Singh, *Digital Defense: A Cyber Security Primer* (2015) Springer Press, NY

The essential problem is that people understand that computers can be hacked and that one should have antivirus and firewalls for their computers as they access the Internet. There is not the same awareness that smart phones are essentially wireless computers and that they are indeed quite vulnerable to attack by cyber-criminals. It is first and foremost an issue of cultural awareness that all forms of digital access to the Internet via whatever means—and especially via wireless—tend to be hackable.

There are security measures to protect wireless systems such as those outlined above that can provide a higher level of security. Further wireline, coaxial cable and fiber optic connections can also be compromised. Thus, no network is absolutely secure.

As we move from wireless access by smart phones to the Internet of Things, and to the Internet of Everything, the vulnerability grows exponentially. The ability to protect one's privacy, one's assets that are accessible electronically, or any type of data that is stored on a database somewhere are all increasingly vulnerable.

There is also the belief that the manufacturers of smart phones can create software to protect against hackers gaining access and the belief that if one goes only to https sites—where the "s" in https stands for secure—that one is fully protected. Again, neither belief is correct. There are vulnerabilities—especially via installed apps—that make smart phones vulnerable. Also, hackers can create counterfeit https sites that are not only not secure but are also traps for the unwary.

The warning was made decades ago that someday we will pay more money to protect against cyber-attacks than to have access to the information itself. This is clearly becoming truer every day.

The bottom line is that wireless smart phones, wireless routers, wireless Wi-Fi systems—even if they are password protected—are increasingly vulnerable to attack. In a home one is much safer to directly connect via a hardwire connection than a wireless router. On a cell phone it is best to use it to simply access it for messaging, phone conversations, and general information. This means do not access your bank account, brokerage accounts, or send or receive messages that might include your credit card number or private IDs. It may be inconvenient to resist, but it is truly the safest way.

Many large corporations now use tele-workers who perform their jobs from their home and use wireless routers to perform their work on private and confidential virtual private networks (VPNs). There are other companies that operate confidential networks within an office using password protected Wi-Fi wireless systems, without adequate security in their passwords, or even a system to find out if all the "registered users" are current and limited to authorized users. A security audit of such wireless networks—as well as hardwired networks—is highly recommended.

And the security problem is not just with private or corporate networks trying to protect trade secrets or vital customer information such as credit card data. This is a huge problem for governments at the local, state and national level. Governmental entities own and operate many wireless LANs and Supervisory Control and Data Acquisition (SCADA). If these networks—especially wireless networks—are operated with little or no sophisticated protective passwords that are frequently updated this can have very bad results. This is true for many different reasons. Wireless LAN

networks, SCADA systems, and Wi-Fi networks are often operated with the passwords provided by the equipment supplier and are never updated. Governmental agencies often have budgetary limitations for the information and communications technology operations, and security expenditures are often the first to be cut over operating unit demands for new, retrofitted, or outdated networking systems equipment.

Another frequent problem is that different departmental units have different procedures, standards and security protocols, and the operating units in local governments that are responsible for transportation, water, sewerage, power systems, etc., are not expert in security systems, standards or procedures. A cyber-terrorist only needs to probe to find where the weakest link might be. In one community it might be in traffic signal controls, in another it might be in water and sewerage systems, in yet another it might be in how vital tax records are secured and accessed.

Arlington County, Virginia, was selected to be in the top seven cities in the world in the Intelligent Communities competition held annually by the Intelligent Community Forum. When the Information Technology Advisory Committee examined the security, codes related the Supervisory Control and Data Acquisition (SCADA) systems that included wireless access systems, such as for the traffic signaling system, it was found that five different departments were responsible for overseeing and assigning security codes for these systems, and the level of security was quite low.

In the case of Arlington County this problem was corrected by assigning the security protection process to a single entity, the Department of Technology, with strict controls and a particular competency in this area. Further an independent audit of the security process for both wired and wireless-based is now carried out annually to ensure that security processes and updated codes were quite well protected. The point is that this vulnerability was detected in one of the wealthiest, most highly educated, and most technically sophisticated communities in the United States. This suggests that this particular problem is likely widespread across the United States and many other countries around the world. Cybersecurity of wireless industrial controls for urban infrastructure is of particular concern. The issue of SCADA security and vulnerability to attack is addressed in greater detail in Chap. 8.

There are serious and widespread problems of wireless system security as well as operational connectivity and functionality that constitute a major concern across many different systems at the local, state, national and even international level. Thus, these concerns go well beyond the security associated with the personal use of smart phones by individuals or by wireless systems controlling SCADA industrial control networks. There are wireless systems that are used by police, fire, EMT first responders, and by armed forces where there are problems of interoperability, security or functionality.

In the United States one solution that is being pursued is known as wireless priority service (WPS) WPS is a priority telecommunications service that improves the connection capabilities for authorized public safety and national security and emergency preparedness (NS/EP) cell phone users. An emergency call using WPS will be given priority in the call queue for the next available channel. WPS calls do not

Fig. 7.1 The broadband FirstNet System has been designed by first responders. (Graphic courtesy of the Department of Homeland Security)

preempt calls in progress or deny the general public's use of the cellular network. The authorized users of WPS in the United States can range from senior members of the presidential administration to emergency managers and fire and police chiefs at the local level, public health employees, to critical technicians in wireline and wireless carriers. This usage is also possible for those in critical sectors of the economy such as banking, energy, transportation and communications, nuclear facilities and other vital national infrastructure. Commercial service providers and, in the United States, current service providers include: AT&T, Cellcom, C Spire, GCI, Southern LINC, Sprint, T-Mobile, U. S. Cellular, and Verizon Wireless. Similar options are available in other parts of the world. It is worth spending some time doing research to find out what is available in your country or region.[5]

On February 22, 2012, the U. S. Congress enacted the Middle Class Tax Relief and Job Recovery Act of 2012 (Spectrum Act) that, among other things, directed the Federal Communications Commission to allocate the D-Block (758–763 MHz/788–793 MHz) to public safety for use in a nationwide broadband network. The purpose of this allocation was to create the First Responder Network Authority (FirstNet) as an independent authority within the U. S. Department of Commerce. FirstNet is charged with responsibilities for deploying and operating the nationwide public safety broadband network and will hold the license for both the existing public safety broadband spectrum (763–769 MHz/793–799 MHz) and the reallocated D Block as noted above. In this same law Congress also allocated up to $7 billion to FirstNet to construct this nationwide public safety broadband network. (See Fig. 7.1.)

[5] Frequency Asked Questions about Wireless Priority Service, https://www.dhs.gov/wps-faq August 2017.

Today, some 7 years later, this broadband first responder network system is now in various stages of implementation with some 15 states specifically opted into this program and all of the states developing plans for review. In addition to this system being broadband in its design and engineering it is also secure in terms of its cyber architecture. As such its design can be considered as one that might be considered for smart cities around the world.[6]

Most smart cities around the world that are being designed and implemented include a modern and highly responsive first responder network that is broadband and secure. This is no small issue to consider. There is first the matter of a suitable allocation of spectrum to allow the creation of a broadband first responder system. This is increasingly difficult in light of the accelerating demand for spectrum to accommodate consumer demand for broadband mobile wireless services that include video services. It is also demanding in terms of meeting all the demands for police, fire, health services and other first responder needs.

Conclusions

The considerations associated with broadband wireless services are demanding in almost every conceivable context. There is first the problem of accommodating runaway growth around the world. The expansion from data to voice to video-based wireless services and now universal access has made the problem of finding sufficient spectrum to accommodate consumer demand around the world very difficult. Keeping separate spectrum to just accommodate the needs of first responders represents a quite demanding challenge.

Clearly all such types of mobile networks should have a high degree of cybersecurity, and the very aspect that these networks are wireless and mobile makes them subject to interception. Further the popularity of mobile networks and the exponential growth of applications and of instant pay systems have given rise to additional problems of cybersecurity.

On one hand the smart cities of the future will seek the convenience of mobile wireless systems that will likely include terrestrial, satellite, and even high-altitude platform systems, but on the other hand contain a high level of cybersecurity against criminal and techno-terrorist attack. This particularly applies to the needs of police, fire, public health, EMT, and infrastructure-related personnel that are required to respond to major natural disasters or in the event of a significant cyber-terrorist attack. Smart and flexible frequency allocations, advanced encryption, and a good deal of backup with redundancy of key infrastructure (i.e., fiber optic cables, broadband wireless systems, high-altitude platform systems, satellite networks, power networks and emergency power systems) will all be reflected in the smart cities of the future.

[6] Federal Communications Commission FCC White Paper. The Public Safety Nationwide Interoperable Broadband Network: A New Model for Capacity, Performance and Cost http://transition.fcc.gov/pshs/docs/releases/DOC-298799A1.pdf June 2010.

Chapter 8
Smart and Safe Control Systems for the Smart City

The increased automation of key urban infrastructure via such means as Supervisory Control and Data Acquisition (SCADA) networks and Artificially Intelligent Industrial Command and Control Systems adds convenience and reduces labor costs and urban government employment needs. But, alternatively these automated control systems have dramatically increased the number of potential vulnerability points in cities. In short, as artificially intelligent command and control capabilities are introduced into smart cities it also means disgruntled employees, cyber-criminals and cyber-terrorists can attack vital urban infrastructure. Instead of attacking vital infrastructure physically they can attack the electronic brains that control the infrastructure these cyber-criminals and terrorists wish to attack.

These assaults no longer have to be physical and can be carried out a half world away, where identities can be shielded, and capture at the scene of the crime is no longer possible. And it does not have to be terrorists. Someone who is fired from a water purification plant, or the traffic signal control division, or even the tax records department could extract revenge by attacking key infrastructure or destroying sensitive public files.

Noted economist Robert J. Samuelson, in an editorial in the *Washington Post,* has written a number of recommendations about ways to defend against cyber-attacks by hostile nations or various types of cybersecurity attackers. He has said that the focus on the Russian meddling in the U. S. elections has somehow masked the even greater threat of hostile nations having access to electronic command capabilities that could be used to disable national electronic grids, cooling controls to nuclear power plants, or control systems for water, sewage, or rail and vehicular networks. Samuelson has made a number of recommendations, such as creating independent power plants for military bases, creating independent, off-the-net, dedicated control systems for water and sewage systems, traffic control networks, etc.

However, he also notes that such protective measures could be expensive, and no one wants to spend the money needed to increase cybersecurity. A number of his

© Springer International Publishing AG, part of Springer Nature 2019

J. N. Pelton, I. B. Singh, *Smart Cities of Today and Tomorrow*,
https://doi.org/10.1007/978-3-319-95822-4_8

recommendations make sense and deserve study, but what his editorial does not address is that any automated control system can be internally attacked. In the age of AI algorithms and the Internet of Things (IoTs) there is a need to even more sophisticated protections. These will be increasingly focused on the use of "block-chain" security measures that can work at the IoT level for sensors and control systems and the human-machine interface (HMI) to stop potential mayhem that can occur in automated systems.[1]

These cyber-attacks can be made via a variety of malware that includes viruses, Trojans, ransomware or actual physical assaults on supporting energy, communications and IT links or computer components in the automated networks that control traffic networks, water supplies, sewage treatment processes, electrical power distribution, pipelines, nuclear power stations and much more. A strategically placed bomb that is located at a the right location can shut down a city's water supply, cripple an urban traffic signal system, or stop the processing of sewage.

This chapter addresses the various types of vulnerabilities that exist in urban infrastructure, and strategies for protection of these vital systems against spurious cyber commands, malware attacks or other types of physical assaults that might be undertaken. The actual direct attackers of the smart city of the future do not have to be cyber-criminal masterminds but simply petty crooks that may not even realize the scope or nature of their crime. In short techno-terrorist cyber hackers might develop a plan to blow up a vital communications link or local area network (LAN). They could then hire a functionary to put a bomb with a timer or electronic igniter into place without that person knowing that the result of this action would be to shut off all water supply for an entire city.

In this regard the architects and engineers of tomorrow's smart cities will need to exercise great care and more than a little wisdom. The mission of the architects of the key urban infrastructure of the future must do more than to create efficient and highly functional infrastructure that is reliable, low in energy consumption and polluting effects, cost effective, easily repairable and updatable in terms of future improvements. Perhaps the top design criteria is to create smart control systems that are protected against cyber-attacks, able to detect intrusions, isolate infected control systems, and restore systems to normal operations with maximum efficiency.

Over centralization of network controls seems to be a caution to be taken particularly seriously. Network design to create sub-networks that can be activated and begin functioning if the centralized controls should fail—either due to natural disaster, component failure or attack by hackers or techno-terrorists. The design of the control systems must particularly consider that there are dangers that go beyond cyber-criminals and terrorists. As will be seen below chief information officers (CIOs) recognize that there is always significant threat to computer-controlled networks that can come from natural disasters and component or unit failures. These type of emergencies can also disable or limit operations of automated networks.

[1] Robert J. Samuelson, "Another Huge Threat from the Internet" *Washington Post*, March 26, 2018, p. A17.

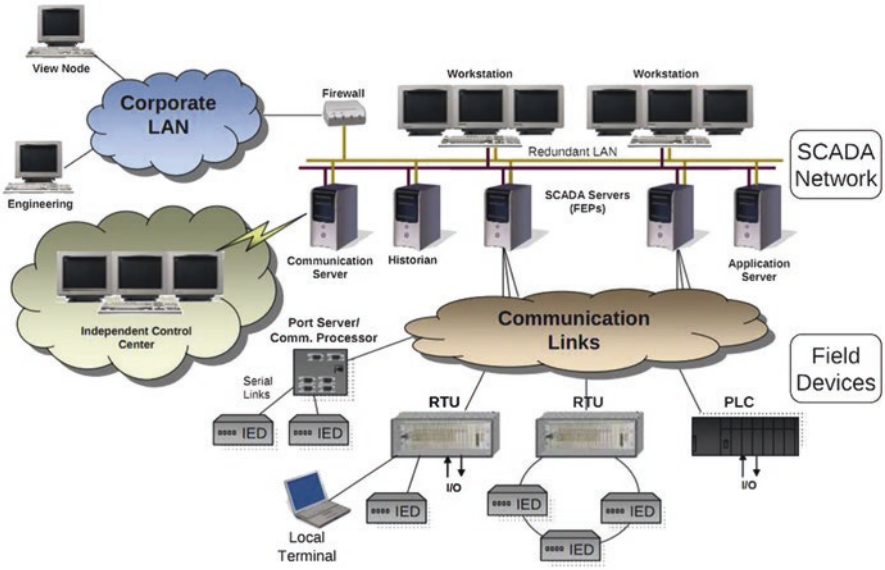

Fig. 8.1 Key communications and computer components of a representative SCADA network. (Source: Pacific Northwest National Laboratory)

Designing Failsafe SCADA networks

Industrial control systems for key infrastructure are most typically configured in the form of SCADA networks, and there are vulnerabilities in both the communications systems that can be wire- or wireless-based and in the computer systems and the associated software. Most attention is usually given to the computer hardware and software vulnerabilities to things such as the Stuxnet virus that was used to attack the Iranian nuclear weapons development program. It is important to recognize that the communications systems can be used to terminate or misroute control commands.[2]

Figure 8.1 clearly shows that a representative SCADA network that is well-designed has redundant communications links, typically in the form of local area networks (LANs) and in the case of very large geographic systems such as control systems for pipelines, wide area networks (WANS). It might be prudent to have as backup satellite links that can be activated instantly on demand with emergency codes in the case of the failure of a particular industrial system controlling vital infrastructure.

There could even be a more sophisticated design within a SCADA and its LAN operation, particularly when it is conveying commands for vital switches and network operation within a key infrastructure. This type of additional layer of security might require a confirming coded message at intervals that provides an additional

[2] InfoSec Institute, Improving SCADA System Security, Dec. 6 2013. http://resources.infosecinstitute.com/improving-scada-system-security/.

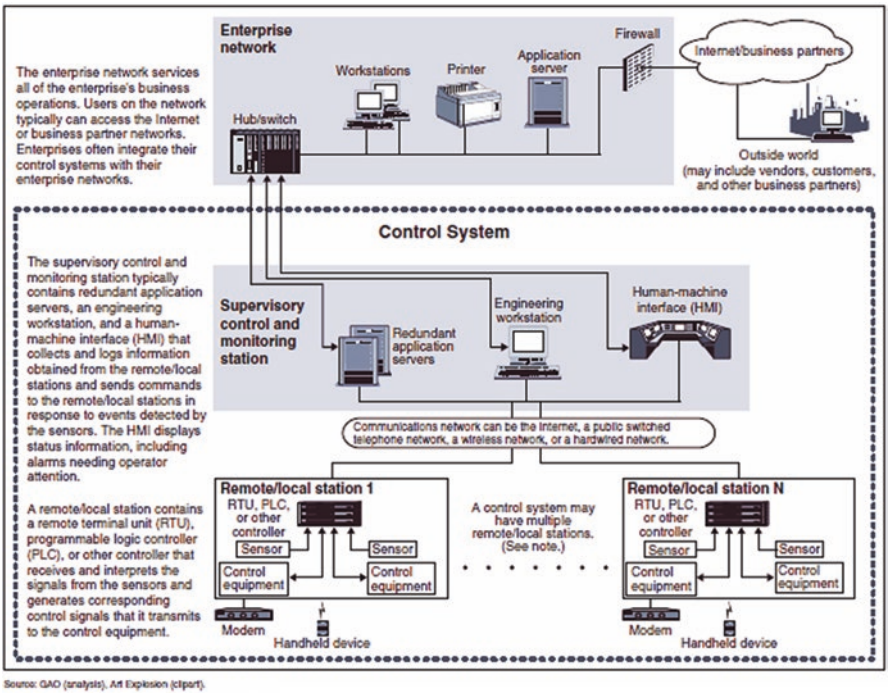

Fig. 8.2 The importance of HMI within a supervisory control and data acquisition (SCADA) network. (Source: U. S. General Accounting Office)

level of security. The key here would be a backup if the system providing the confirming codes should break down. This type of system was employed in the case of the Intelsat satellite system whereby commands to satellites required a confirmation from another remote site.[3]

It is impossible to anticipate all types of things that can either fail due to equipment or electrical or communications malfunction, or natural disaster, or criminal or terrorist attack. This is why the human-machine interface is so very important to combatting and responding to cyber-attacks. The HMI display station provides vital information to the operators of SCADA networks. It alerts human operators to the need for responses to signals by indicating errors or a need for corrective answers, repairs or other responses. These data acquisition return signals can alert the operator not only to things such as pipeline leaks, pumping station equipment failures, and sewage pipe blockage but also signal cyber-attacks to the SCADA software. Although there are algorithms that can be developed to respond automatically to most of the various SCADA alerts to errors and network problems, it is key to detect them quickly and also to carry out quick corrective action. Thus for the HMI station

[3] Joseph N. Pelton, *Basics of Satellite Communications* (2006) 2nd Edition, Chicago, Illinois, International Engineering Consortium.

it is always important have human operators in the loop, even though AI algorithms might be designed to alert the operators that there are problems with the SCADA software or that incoming signals may very well be indicators of a cyber-attack.

Figure 8.2 shows the critical role that the HMI plays within a SCADA control system and why it needs to be the focus of any cybersecurity design exercise. Such security considerations include backup communications to and from the HMI, operators trained in ways to detect cyber intrusions and procedures to respond quickly to all forms of cyber-attack.

Current SCADA systems, despite security upgrades, still could continue to exhibit a number of potential vulnerabilities. The most common cyber-attack methods on SCADA systems are:

- back doors and holes in network perimeters
- attacks by disgruntled employees
- vulnerabilities in common protocols
- attacks on field devices through cyber means
- database attacks
- communications hijacking or LAN shutdown or man-in-the-middle attacks.[4]

Another top consideration here is how to avoid over centralization of SCADA network design as opposed to having some form of decentralization so as not to shut down a vital infrastructure all at once and allow better understanding of from where cyber-assaults have been launched and create a greater ability to isolate the effects of such an attack or system failure.

Efforts have been undertaken to consult with system operators and chief information officers to determine their security concerns and steps that might be taken to enhance the security or improve the performance of a SCADA network by appropriate protective measures. The result of this effort is reflected in Table 8.1, with the steps being prioritized by frequency of response from Step 1 as the most frequent response to Step 21 as the least frequent. It is important to note that addressing natural disasters was only 19th out of 21 steps, but that in fact this must be considered as a likely occurrence and that concerns about mechanical and electrical breakdowns or failures and natural disasters, such as a coronal mass ejection (CME) that could create a major hit on the electrical power grid, should be considered a much higher priority.

There is no single universally accepted set of standard practices with regard to SCADA security. There are, however, a number of logical guidelines that have been accepted and represent useful references that should be consulted. A listing of some of the most widely respected guidelines in this regard is provided in Table 8.2.[5]

---

[4] Bonnie Zhu, Anthony Joseph, and Shankar Sastry, *A Taxonomy of Cyber Attacks on SCADA Systems.* (2011) ACM Digital Library, https://dl.acm.org/citation.cfm?id=2085202 (Last accessed Oct. 29, 2017).

[5] "Cyber Security: New Challenges for SCADA and Industrial Control Systems," White Paper # 2, Global Institute for Security and Training, 2013.

Table 8.1 Recommended steps to secure SCADA systems (Source: The President's Critical Infrastructure Protection Board & U. S. Department of Energy SCADA Security Recommendations)

21 steps to improve cybersecurity of SCADA networks	
Step	Description
1	Identify all connections to the SCADA network.
2	Disconnect unnecessary connections to the SCADA network.
3	Evaluate and strengthen the security of any remaining connections to the SCADA network.
4	Harden SCADA networks by removing or disabling unnecessary services.
5	Do not rely on proprietary protocols to protect your system.
6	Implement the security features provided by device and system vendors.
7	Establish strong controls over any medium that is used as a backdoor into the SCADA network.
8	Implement internal and external intrusion detection systems and establish 24-hours-a-day incident monitoring.
9	Perform technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns.
10	Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security.
11	Establish SCADA "Red Teams" to identify and evaluate possible attack scenarios.
12	Clearly define cybersecurity roles, responsibilities and authorities for managers, system administrators and users.
13	Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection.
14	Establish a rigorous, ongoing risk management process.
15	Establish a network protection strategy based on the principle of defense-in-depth.
16	Clearly identify cyber security requirements.
17	Establish effective configuration management processes.
18	Conduct routine self-assessments.
19	Establish system backups and disaster recovery plans.
20	Senior organizational leadership should establish expectations for cybersecurity performance and hold individuals accountable for their performance.
21	Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.

Cyber Security White Paper (2007) The President's Critical Infrastructure Protection Board & U.S. Department of Energy SCADA Security Recommendations

The protection of an urban industrial control system is something that must be designed from the outset. This effort, which draws key steps from the standards noted in Table 8.2, involves the use of at least four critical processes. These processes can be described as Digital Forensics; Engineering, Architecture and Design; Continuous Operational Monitoring; and Ongoing Vulnerability Management. Figure 8.3 depicts the way these processes are utilized to protect urban and industrial infrastructure operation on an ongoing basis and to test security against future attacks.

Table 8.2 Cybersecurity standards developed for SCADA and industrial control systems

Standards for security risk assessment for SCADA systems
1. API Standard 780 Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries (Adopted by American Petroleum Institute, May 2013)
2. COBIT 5 Business Framework for the Governance and Management of Enterprise IT (Adopted by ISACA, November 2013)
3. ISO/IEC 27000 series collection: Information Security Management Systems (Adopted by the International Organization for Standardization)
4. ISC-CERT Improving Industrial Control Systems Cybersecurity with defense in depth strategies (Adopted by ISC-CERT, October 2009)
5. NIST Security and Privacy Controls for Federal Information Systems and Organizations, National Institute of Standards and Technology (NIST), Adopted, April 2013
6. NIST Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology (NIST), Adopted, April 2013
7. NIST Information Security Handbook: A Guide for Managers, National Institute of Standards and Technology (NIST), Adopted, March 2007

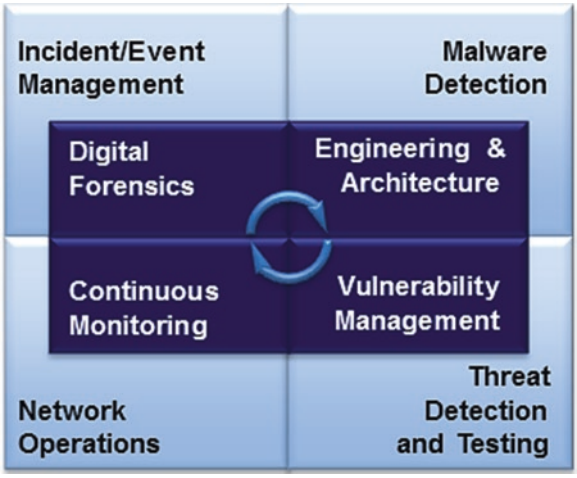

Fig. 8.3 Four processes for protection of industrial controls for vital infrastructure. (Source: Global Institute for Security and Training)

Details of how these processes help to protect network operations, support threat detection and testing, and are critical to malware detection and incident and intrusion management are discussed below.

Digital Forensics

Digital forensics must be constantly applied in order to analyze and understand the meaning of incident reports regarding both intrusions and event management outcomes. This process relates to more than detecting and reporting accurately on all

"in-house" cyber-attack incidents and how these events are managed. This process, if done well, extends beyond keeping aware of all attempts around the world to penetrate industrial control systems via cyber-attacks or even system failures due to natural disasters or mean-time-to-failure (MTTF) of key components and network hardware. Digital forensic reports should indicate why and how such attacks or failures occurred, successful preventive measures, or expose harmful network penetrations. This ongoing analysis of attacks should cover not only internal intrusions but also information about attacks or failures that occurred elsewhere as well. This is critical to preventing further attacks and creating better protection via network security upgrades. Digital forensics should produce reports on attempted cyber-attacks, how they were deterred, and new types of tools or methods that might better defend against future cyber-assaults. Key to successful digital forensics is the creation of a better process to share information about the nature of cyber intrusions and how they can be stopped successfully.

Engineering, Architecture and Design

Any urban or industrial infrastructure that is designed for 21st century operations must be designed to be resilient against cyber-attack and detection of all sorts of malware of any type that can attack databases, IT networks or communications systems, either directly in real time or like Trojans that might be activated at a later time. The hardware and software must not only be designed to protect against malware attacks, but it also must be designed with enough flexibility and modularity so that the control software and hardware can be upgraded and improved over time. The design should also be flexible so that any malware attack can be compartmentalized and contained or isolated until repairs are made and normal service is restored. Possible design elements include secret authentication features that are isolated from most system operators and are based on key functions requiring approvals from top management. There also could be delays in some execution of control commands with alerts to high level supervisors before implementation unless verified by an additional security code.

Such authentication systems would be most protective against cybercriminal or techno-terrorist attack if they can be executive from a more location. The trouble with such authentication code verification can is if there is a communications or component failure or a supervisor who is suddenly unavailable, blocking a critical valid control command. Such systems require extra redundancy, and no system can ever be failsafe despite what design engineers might claim.

Continuous Monitoring

Continuous monitoring is vital to successful network operations of any type of industrial or urban infrastructure, regardless whether this is for transportation, energy systems of all types, communications or IT systems, water and sewage systems, etc. SCADA systems not only exercise supervisory control but also provide vital data acquisition to ensure that network operations are as they should be. Continuous monitoring must not only examine incoming data to ensure that networks are performing normally but are also built to detect spurious data providing incorrect information. Thus continuous monitoring might include random coded signals that require a proper authentication response to verify that it is live data coming through rather than "faked" readout such as simple repeats of previous data reports. In short, continuous monitoring at the human-machine Interface must involve more than passively awaiting problem alerts. Some form of diagnostic authentication system needs to be a part of the continuous monitoring systems of the future.

Vulnerability Management

Threat detection and testing of end to end systems is vital to the safe and reliable operation of a smart industrial control system. Vulnerability management includes not only executing a successful response to block an attempted intrusion but is an active process of continuous monitoring and testing to make sure that operations are indeed normal and that incoming data is not being synthesized by a cyber-attacker. This verification process either involves active testing or authentication of incoming data via coded messaging, algorithms that detect abnormal data, or other testing processes. It is also important to study reports of intrusions from other operational networks and to consider case study reports concerning lessons learned from cyber-attacks that have utilized new and improved techniques, software or hardware to stop cyber-attacks against parallel systems.

Learning Through Experience and Case Studies

Case studies on successful attacks on SCADA networks are always instructive. Lessons from such case studies around the world lead to very useful conclusions about better cyber-defense of industrial and governmental infrastructure.

1. Numerous case studies confirm that many attacks come via wireless LAN connections to SCADA systems. The bottom line is that wireless LAN connections to vital infrastructure should be limited, and to the extent some access to vital infrastructure is allowed stringent security should be enforced. This would mean that

such wireless LANS would not only be password-protected by highly secure passwords (i.e., perhaps 15 characters or more with enforced use of symbols, upper and lower case letters and numbers of a random nature). These passwords would be changed periodically, and security audited by a third party. In the future there could be other measures such as retinal scans, face recognition scanning, etc.

2. Computer equipment and telecommunications switches that have back door access via manufacturer codes should have these codes changed before installation into infrastructure networks. It is often disgruntled former employees, especially if fired for cause, who know the back door codes that are in some cases used to sabotage a telecom, IT or other such network. This strongly suggests the need for a change of access codes periodically, and especially when an employee is discharged, or the spouse or relative of an employee is fired. The bottom line is that trusted employees should be entrusted with access codes. In super secure facilities such as nuclear power plants, etc., it might be important to consider having two employees with authenticating codes being entrusted with assuming control of vital infrastructure.
3. Directed denial of service attacks are becoming ever more sophisticated, and via the Internet of Things can assemble millions of attacking processors. The latest in protective software for withstanding such attacks now needs to be used to ensure that Internet-accessible sites can survive such cyber-assaults.
4. Buses and other first responder vehicles can be equipped with override capabilities to trigger traffic light signals. Other "intelligent" traffic systems are designed to reverse all traffic signals to green to evacuate a city in an emergency. The potential for abuse of such systems have been shown in popular movies such as *The Italian Job.* There is thus merit in having algorithms that do not allow control commands such as turning all intersection lights green, or other highly unusual commands, except with coordinated high-level authentication codes. Similar use of such authentication codes and AI algorithms with regard to water and sewage systems, banks of elevators and escalators, fire-fighting sprinkler systems, and especially nuclear power plants and their safety systems would be particularly recommended.

Conclusions

The number of vital SCADA systems that are in charge of traffic signal systems, banks of elevators, water and sewage systems, pipelines, electrical power transmission systems and transformers, security monitoring systems, credit card authentication systems (for parking meters, parking lots, parks, etc.) communications and IT systems, etc., continues to grow. The addition of Internet of Things (IoT) devices to such systems can on one hand add additional functionality to these vital infrastructures, but at the same time it greatly increases the access points by which cybercriminals or techno-terrorists might initiate a digital assault.

There are many defensive systems to prevent unauthorized cyber-attacks. Access codes, dual authentication systems, smart algorithms that do not allow dangerous activities with regard to dams, bridges, traffic signals, power plants, energy grids and more without the highest level of authorization and multiple authentication codes can be used to prevent abuses of smart infrastructure.

Defensive systems can only go so far to protect digital networks and modern urban infrastructure. At some point proactive cybersecurity systems will need to find the cyber-criminals and techno-terrorist attackers and bring them to justice. Changes to the Internet architecture and controls on the Internet of Things (IoT) as it becomes the Internet of Everything (IoE) may be necessary. Likewise efforts to probe the dark web and bring some form of controls to electronic monetary systems such as bit coin may also become necessary. This is no simple or easy task. Personal freedom and liberty from government surveillance are keys to democratic processes. It may well be that clever technological solutions may be found to the problems that come with more and more automation in 21st century society.

Chapter 9
The Smart City Floating Safely on the Cloud

One of the most significant changes in the world of cyber systems has been the development and meteoric rise in the processing and storage capacity of the cloud. The mushrooming of the capabilities and use of the cloud—no pun intended—coupled with the development of the Internet of Things (IoTs) and the new features for broadband fifth generation wireless services will create fantastic new capabilities. But these enchanced digital tools will but give rise to new levels of cybersecurity concerns and potentially create new vulnerabilities with regard to vital urban systems and especially critical infrastructure.

Much of this new broadband networking and communications capability will in the near term be driven by video services—particularly for mobile services. But in the longer term it will not be person to person services that will the prime source of expanded broadband networking demand. Instead, people will be increasingly out of the loop. The increased presence and use of IoT-enabled devices will inevitably lead to a spike in machine-to-machine (M2M) messaging. Further, artificial intelligence related-processing and control systems, plus decision-making and robotic control systems will also drive further demand. In short, these automated tools will lead to a more and more automated world.

This huge increase in incoming and actionable data will combine to ramp up the demands made on the cloud for both data storage and processing—and at an exponential rate of expansion. Thus, of all the key pieces of infrastructure that define the smart city of the future it will be broadband networking that will constitute its quintessential feature. The effective meeting of the demand for vital networking services and the secure storage of the information sent through these networks will increasingly depend on secure cloud infrastructure and services. Thus, the provision of broadband networks and secure cloud services will be inextricably linked within the design, engineering and operation of the smart city of the 21st century.

© Springer International Publishing AG, part of Springer Nature 2019

J. N. Pelton, I. B. Singh, *Smart Cities of Today and Tomorrow*,
https://doi.org/10.1007/978-3-319-95822-4_9

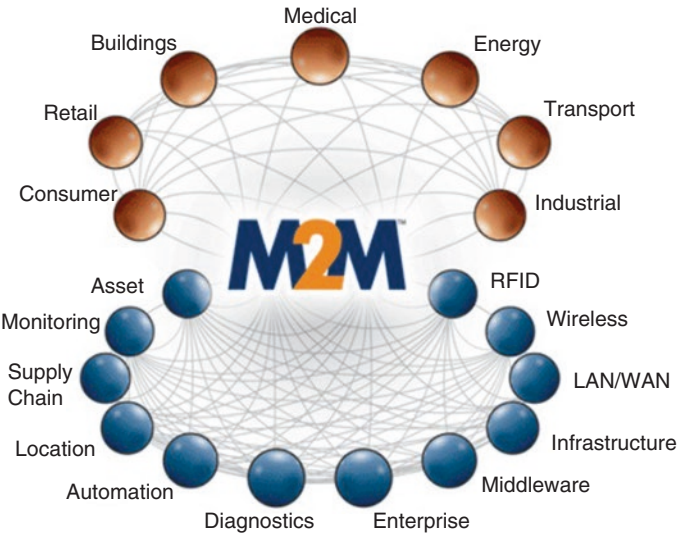

Fig. 9.1 Machine to machine data relays will support many key services and an array of urban infrastructure. (Illustration courtesy of Digital Defense, Inc.)

Current estimates are that IoT-connected devices and machine-to-machine communications will expand 15 times in the next 4 years, from 2018 to 2022. This promises to fuel the growth of cloud-based services at ever faster speeds.[1]

Other developments related to social media, IoT, 5G wireless services and more will also contribute to this incredible surge in digital networking growth. This rapid rate of expansion of applications throughout industry and society suggests an explosion across digital data banks stored on the cloud, ballooning broadband transmission rates for digital communications and greatly expanded use of virtual reality. The use of virtual reality and 3D imaging will likely occur in almost every sector ranging across games, education, training, medical applications, transportation, energy, consumer services and sales, buildings management and engineering, and indeed all aspects of industry.

Yet this increase in data transfer rates has three key implications. One implication is the exponential increase in data flows. The second is that this staggering increase in data flows will require digital processing machinery to cope with the sheer volume of data. The third implication is that the sharp spike in data flows to cloud providers and their supercomputer processors. There are cyber-risks during data flows to and from the cloud and even risks of theft or manipulation as data is stored within the cloud. (See Fig. 9.1.)

Some believe that the cybersecurity provided by well-established and sophisticated cloud providers can provide much higher levels of security than that of smaller

[1] The Internet of Things for Defense, A White Paper, Wind River—An Intel Company, October 2015. http://www.windriver.com/whitepapers/iot-for-defense/wind-river_%20IoT-in-Defense_white-paper.pdf.

companies and that they should therefore transition their operations to the cloud. Yet there remain key questions. Do data centers and networks run by cloud providers feature a greater level of security than what most enterprises can achieve on their own? Even if cloud systems do have a high level of firewall protection, is there not always the potential of cloud employees with access to data to have unauthorized or felonious access to vital information?

These are key questions that all chief operating officers need to consider. Charles Phillips, CEO of Infor, for instance, says his firm believes that the transfer of data operations makes a good deal of sense and is urging his clients to move into the cloud at an aggressive pace, now that he believe off-premise security concerns at least with top-level cloud service-providers are no longer the issue. "In the old days, companies were more concerned about the public cloud not being secure," said Phillips. "Today, most of their security breaches are internal".[2] Others, as discussed below, still have concerns and have approached the use of the cloud with caution. Yet other enterprises of sufficient size and resources have responded to the challenge by creating "private clouds" behind their own firewall.

It is important to note that this involves not only investment in specialized software and hardware, plus technical skill and knowledge, but also regulatory expertise. In the United States, for instance, there are specific requirements to retain information consistent with the requirements of the Sarbanes-Oxley Act (Pub.Law. 107–204, 116 Stat. 745, enacted July 30, 2002), which was known as the Public Company Accounting Reform and Investor Protection Act in the U. S. Senate as well as the Health Insurance Portability and Accountability Act (HIPAA). This option of creating a private cloud is one that larger smart cities might wish to consider if they have sufficient economy of scale.[3]

These key issues related to the increasing use of the cloud by individuals, corporations, and cities will be examined in this chapter as well as in the following chapter on urban infrastructure.

Coping with Complexity and Increasing Data Rates

The issue of urban security and how to cope with cyber-risk in the smart cities of the future is very much about shooting at a moving target. Complexity of systems, rates of data flows, and interactive systems analysis will all make the issue of cybersecurity more difficult. In considering the security of cloud operations, one must also

[2] Cameron McKenzie "Allaying the AWS security concerns: How the cloud became more secure than on-premise" The Server Side, http://www.theserverside.com/feature/Allaying-the-AWS-security-concerns-How-the-cloud-became-more-secure-than-on-premise. (Last accessed Nov. 2, 2017.)

[3] Lucas Stewart, "Private cloud computing models alleviate some cloud security issues" The Server Side, http://www.theserverside.com/tip/Private-cloud-computing-models-alleviate-some-cloud-security-issues. (Last accessed Nov. 2, 2017.)

consider the cybersecurity as well as the physical security of data links to the cloud to assess the reliability of one's data operation as well as vulnerability to cyber-attack.

There are several levels of concerns here to consider:

- *Attack on the Security of Databases via a Cloud Operation.* In this case one must consider the security of information that is stored on cloud systems and possible ways that it might be vulnerable to attack and how the accumulation of truly massive amounts of data at a single location might make it much more the focus of techno-terrorists or cyber criminals.
- *Attacks on Processing Systems and Algorithms:* A second aspect to consider is that there might not only be attacks on stored data in cloud systems but also on the processing systems operating on cloud-based systems.
- *Vulnerabilities of Automated Networks Directly Linked to the Cloud:* A third aspect to consider is the complexity and vulnerabilities that the Internet of Things and the future Internet of Everything will add to the world of processing. There is now an exponential rise in machine-to-machine (M2M) communications. This leads to automated systems designed to protect against distributed denial of service (DDoS) attacks. Further there are more and more systems globally that are controlled by automated industrial control systems such as SCADA networks. This leads to more and more automation of systems and creates vulnerabilities that might be hard to detect and recover from quickly. (This issue is largely addressed in the following chapter.)
- *Everything in One Basket:* Cloud operations are becoming a potential omnibus target for terrorists or the cause of a mega-disaster due to system failure or natural disaster. The fourth key consideration is that databases, software and processing systems vital to the operation of more and more critical infrastructure—of all types—are now loaded on the cloud. A recent advertisement for the IBM cloud noted how their operations were vital to aircraft in the sky, operation of train and subway systems, banking transactions, and much, much more. Here the issue is not only that of possible intrusions and attacks on cloud operations by terrorists, but also natural disasters and systems failures (i.e., power, communications, network connections, and more). Any of these possible types of failures could disable vital functions that now depend on cloud-based services and operations. In short aircraft in the skies, train operations, a nuclear power plant or the operation of elevators or air ventilation systems in skyscrapers around the world are now vulnerable at a single area of attack—or failure. One does not have to be anywhere close to these critical areas for catastrophic failures to occur. One only has to be able to attack cloud-based computer operations, or a natural disaster or fire to occur, for a cloud-based failure to have catastrophic consequences.

All four of these concerns are of significance and are considered in this chapter and the next.

The expanded capabilities of the cloud will increasingly expand from industry applications into more and more consumer-based uses and most important to this book into the control and optimization of vital urban infrastructure. Thus, the vastly

expanded capabilities of next-generation clouds will intersect with expanded use of social media, virtual reality in consumer goods and services, IoT devices in homes, schools, hospitals, and governmental systems of all types. It will expand by perhaps over a hundred times within a few decades. The making of more and more appliances, devices and infrastructure both smarter and able to communicate will give us an entirely new vision as to the capabilities and "mission" of homes, offices, neighborhoods and cities of the future. Unless a concern and caution for cybersecurity is designed into these new digital communications, processing, and control systems, digital vulnerabilities will only grow.

Today the greatest percentage of use of the cloud is in industry and defense-related applications. Within a decade it will have enormously expanded to become almost omnipresent in governmental infrastructure and related applications and services as well as prevalent in consumer devices and usages. When a person goes to school, plays a computer game, gets on an elevator, rides in a vehicle, makes use of a utility such as water, gas, electricity, or passes through a traffic light he or she will not only become interactive with an IoT-enabled device, the person will also be using what might accurately be described as interacting with the "super cloud." These clouds will have their storage capacity measured not in terabytes or petabytes, but perhaps within a decade measured in yottabytes (i.e., 10^{24} bytes). The processing power and storage capability that will be available will be limited only by the broadband network accessibility that will connect users to these vast digital utilities.

Already smart consumers are using consumer-based cloud services such as Dropbox, Google Drive, Apple iCloud, Microsoft OneDrive, Box, ZipCloud, Just Cloud, MyPCBackup and other such services to store safely and more securely their computers' vital records and personal communications. These services are perhaps as vital if not more so than their subscription to anti-virus or firewall services and typically also cost about the same, i.e., from $2 to $10 per month. Increased visualization, more IoT smart devices that are collecting and distributing data and more will make cloud back-up and encrypted storage of data ever more important.

These exponential changes in data collection, storage and analysis portend a dramatically different future that will impact every aspect of life in the smart cities of the future. These changes will be reflected in a myriad of ways. We will see increases in the speed, volume and pervasiveness of machine-to-machine communications and the expanded use of AI algorithms that will cope with streams of data much too large for humans to process. As the sage Arthur C. Clarke reminded us: "Humans are carbon-based bi-peds that process information at 64 bits/second. This means that we would need to live many thousands of years to process petabytes, let alone yottabytes of information."

These profound changes in the nature of digital networking and the expanded use of smart machines throughout society will be experienced on a global basis. These changes give rise to many questions that impact the effectiveness of cybersecurity systems and public safety.

Such questions lead to major concerns about not only the ability of cloud systems to keep up with demand but even more critical questions about how to provide effective and resilient cybersecurity for what will be an increasingly automated

society. The key will be to reap the benefits of such automation while insuring public safety and effectiveness of cybersecurity systems.

There is concern that the 15-fold increase over just 4 years relates not just to the rise in machine-to-machine communications but also a reasonable index to other increases, such as in cloud-based data storage and processing as well as other digital services associated with a more automated world.

There are many key questions for which there are now no firm answers. Will the evolving smart cities of the future indeed be almost fully automated? Or will key elements remain with human operators in the human-machine interface (HMI) as critical aspects of these urban systems and vital infrastructure in order to ensure fail-safe protections? Are human systems operators for complex urban systems sufficiently competent and able to apply critical "security brakes" on cyber systems when this is needed, such as when well-conceived, lightning-speed digital attacks are mounted? And if human operators are not fully equipped to respond to cyber-attacks does this mean that they must be assisted by artificially intelligent algorithms?

Embedded within all of these questions is the further question as to whether or not most of the critical data, operating systems and software closely associated with key infrastructure and its operation will be stored in and processed within the cloud. If virtually all the vital data, control software, and digital operating systems reside on the cloud, does the cloud become a major source of vulnerability? This implies the further issue as to whether or not depending on a single cloud operation becomes a security issue. Should critical infrastructure operations that depend on key data storage and digital operations derived from the cloud be completely backed up? This would, for instance, likely imply the need for an alternative cloud provider so that automatic preservation of all data, key software and control systems can be accomplished on an instantaneous and continuous basis? Alternatively, it would suggest that key servers and digital processing systems would have to be scaled to sufficient levels in order to perform safely and resiliently, at least for some reasonable period of time, when cut off from access to the cloud in the event of a cyber-attack.

The truth of the matter is that humans tend to favor simplicity. When most people see quite complex equations, processes that involve dozens of steps and hundreds of variables, they ask whether there is simpler solution. The most complex concept about the relationship of energy and mass was shown by Einstein to be $E = mc^2$. The Renaissance mathematician and theorist Thomas Ockham was most famous for his "razor," which essentially says that if there is more than one solution pick the simplest one. In short, simplicity is highly pleasing to most people. The great complexity that is represented by today's megacities with populations of over ten million people requires the acquisition, storage, processing, use and protection of a tremendous amount of information.

The bottom line is that individual people, small organizational groups, small, medium and large businesses, and governmental entities need to cope with an ever-increasing amount of data. Each of these entities has greatly different capabilities and access to different types of resources. Cloud-related services have now been developed to provide scaled services for everyone, from the individual to large corporations. This scaling of service to meet the needs of various people and organizations is

adapted not only in terms of the volume of usage but also so that you can do everything on your own computer, or perhaps access and use only infrastructure, or infrastructure and platforms, or move everything to the cloud to use all three—infrastructure, platforms and software. These various levels of usage are known respectively as: (1) Infrastructure as a Service (IaaS); (2) PaaS (Platform as a Service) (renting everything but the applications); and (3) Software as a Service, which would mean accessing the cloud for your software and applications, data storage, data processing and use of the cloud's platforms and infrastructure for all of these functions, including the encryption and protection of your data and its processing.

Figure 9.2 depicts the five types of devices that can access cloud services and the level of cloud service provided. Figure 9.3 shows the progressive use of more and more types of services that can be obtained, ranging from Infrastructure as a Services (IaaS), Platform as a Services (PaaS), and ultimately Software as a Service (SaaS).

The migration of usage from being self contained with no cloud usage (indicated by blue) to performing more and more functions within the cloud (indicated by gray) is depicted in Fig. 9.3.

This is to say that all of these changes will go together as part of a whole new digital ecosystem. In time, perhaps, trillions of IoT-enabled devices will combine to truly become the Internet of Everything (IoE). This will ultimately require machine-to-machine (M2M) digital communications to perform all of the various functions described in Fig. 9.1.The data storage capabilities and processing power to carry out the various functions, such as location determination, diagnostic assessment, safe and resilient automation, software updates, etc., will require what we characterize as super cloud capabilities.

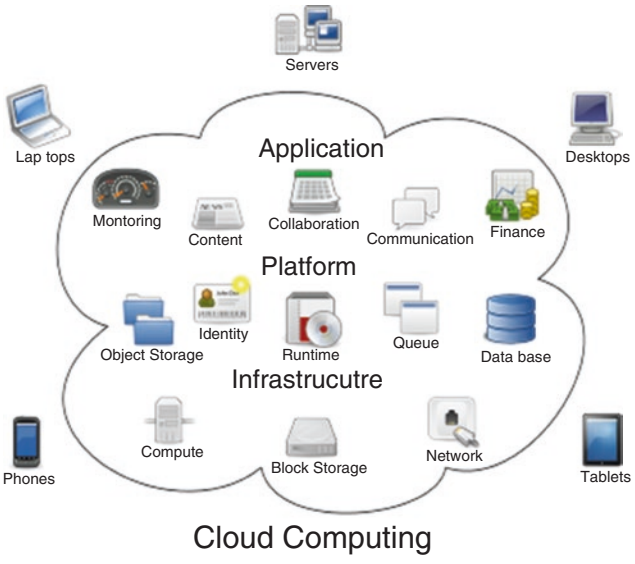

Fig. 9.2 The cloud services are now flexibly arranged for easy access by all types of users. (Illustration courtesy of Digital Defense, Inc.)

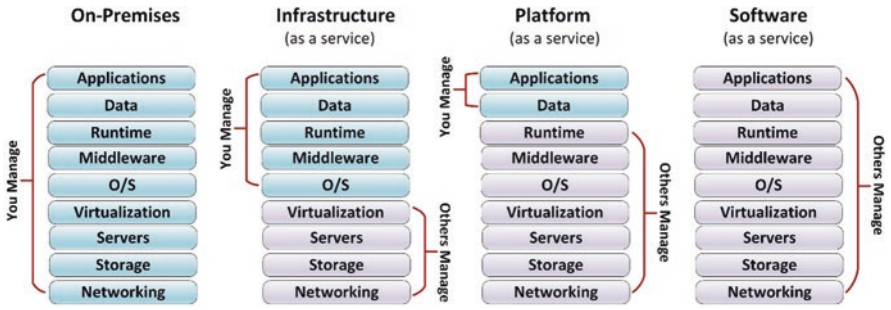

Fig. 9.3 There are many levels of services and facilities available from the cloud. (Illustration courtesy of Digital Defense, Inc.)

Smart City Cybersecurity Concerns and the Cloud

Many people have a simplistic understanding of the potentially complex range of capabilities that they can derive from cloud service providers. In truth one can contract for a great deal of capability from a cloud service provider or a very specific and precisely delimited set of services, applications or infrastructure. Figure 9.3 indicated that one can obtain from cloud service providers various customized options. These can be access to specific infrastructure; or infrastructure plus a platform; or infrastructure, a platform, and software. The details of one's arrangements with a cloud service provider leads to different types of cybersecurity concerns. It is important to understand specifically and in a written contract the degree of separation and "silo-ed independence" that one has in terms of having separately stored and accessible applications, databases, servers, and networking access

Regardless of the level of service provided by a cloud service provider, steps to protect against hacker attacks are important to pursue. One solution that is common is to engage a cloud access security broker (CASB). This can be either a software tool or a contracted service that sits between an organization's on-premises infrastructure and a cloud provider's infrastructure. A CASB role is to serve as a protective gatekeeper Thus a CASB serves a security check that allows an organization with this type of protective shielding to extend the reach of their security policies and system beyond their own infrastructure.[4]

The Equifax mega-hack in July 2017 that is now being investigated by the Federal Trade Commission indicates that even very sophisticated cloud-based services that are assumed to have the most stringent protections against unauthorized access to protected databases are not safe from attack. The key aspect to remember is that use of a cloud does not provide users of this service with any absolute guarantee of cybersecurity. In fact, it actually can expose users to some additional risks.

[4] Definition of a Cloud Access Security Broker. http://searchcloudsecurity.techtarget.com/definition/cloud-access-security-brokers-CABs September 2017.

Conclusions

Cloud services clearly provide cost efficiencies. For smart cities of many different sizes and for smaller and mid-sized business users it allows a number of particular advantages. These advantages include access to economies of scale, and potential efficiencies normally available only to the very largest of commercial users. It can allow for the back-up of key datasets and access to a wider range of processing tools. These cost efficiencies and access to a range of capabilities do come with some potential downsides and risks that were outlined in this chapter. These advantages as well as potential downsides must be carefully considered.

Chapter 10
Challenges and Opportunities in the Evolution of the Internet of Everything

The most significant current trend in the rapidly changing global digital ecosphere is the rapid spread of the Internet of Things (IoT). Indeed, the next iteration in the evolution of the IoTs will be what some are calling the Internet of Everything (IoE). In this new world that includes RFID and digital interface connections with all manufactured and merchandised objects, the world and especially the smart city will increasingly be awash in data that allows instantaneous digital updates on everything. Over time this omnipresence of the Internet and smart-enabled units will expand worldwide. In the world of the smart city virtually every manufactured object will encompass the entire planet and even populate outer space outposts. Wherever there is human activity, electronic networks, or operational satellites the IoE will be there, too.

According to the Information Technology and Information Foundation the global economy is undergoing a profound transformation. This is being driven primarily by the Industrial Internet of Things (IIoT) as it has integrated into almost every aspect of modern life. Thus, the IIoT is now integral to modern engineering, production processes, and virtually every form of economic activity. But while the IT industry will lead most aspects of this transformation, public policy, regulation and standards also will play a critical role in facilitating the adoption and spread of the IIoT as well as controlling abuses and misuse of its capabilities. Legislative reform and regulation must consider and hopefully apply controls related to safety, cybersecurity and environmental impact.

There are huge tradeoffs involved here. On one hand it seems important for reasons of innovation, economic growth and continued prosperity for data to flow freely over the Internet, but this is only half of the equation. On the other side there is a need for effective cybersecurity systems, that workforces are equipped and re-equipped with requisite skills, that safety and environmental standards are enforced, and that small manufacturers and broader supply chains are positioned to adopt IIoT technologies so that they can remain competitive. This is an enormous challenge for the smart cities of the future that extends well beyond IT technology and urban

© Springer International Publishing AG, part of Springer Nature 2019

J. N. Pelton, I. B. Singh, *Smart Cities of Today and Tomorrow*,
https://doi.org/10.1007/978-3-319-95822-4_10

architecture. This challenge is perhaps greatest in the area of effective cybersecurity.[1]

A study by Hewlett Packard into the cyber security vulnerabilities represented by the Internet of Things concluded that 70% of the IoT devices currently in use are vulnerable to cyber-attack.[2] And the problem is that this was Hewlett Packard's assessment as of 2015. Today the vulnerability has increased in terms of sharply increased numbers of IoT devices and the likelihood that the vulnerability—by the percentage of at risk devices—has also increased. Smart cities, smart automobiles, smart appliances, and smart devices of all kinds are all potentially hackable and at risk.

The July 2017 DEFCOM and Blackhat Conferences were jointly held in Las Vegas, Nevada. At these so-called "hacker conferences", there were special sessions related to hacking into cars, car washes, appliances, home and office security systems, camera networks, Wi-Fi nets, and many more IP accessible locations of all kinds. Devices and smart things connected via World Wide Web accessible sites will soar in the years ahead as smart cities—and all that they imply—continue to grow and expand. In the future the question that will be hardest to answer is not what is connected to the Internet but what is not. The problem with the coming Internet of Everything, is that the number of devices connected to the Internet will not be numbered in the millions or even billions but will grow into the trillions.

The reason that one should care about this exponential growth of smart devices is at least twofold. At the first level of concern these hackable IoT devices will increase the risk factor for everyone that drives a car, has a home security system, has a bank or brokerage account, or is linked to a Wi-Fi or IP network. And these vulnerabilities will increase in ways that are overtly obvious and indeed are hidden from view. A cyber-criminal can assume control of an automobile, use a smart refrigerator or a smart security system within a home to access a wireless router to raid one's bank or investment brokerage accounts or to steal medical or embarrassing personal information that can ultimately be used to extort money from unsuspecting victims.

The second level of concern is that the rapid spread of IoT devices can be used as a criminal or even terrorist tool by a skilled hacker. As one key example a cyber criminal can marshal IoT devices to become cyber tools and use as instruments of attack. Accessible IoT devices can be used to create networked bots to undertake Distributed Denial of Service (DDOS) attacks. Any unprotected networked device in one's home could become an instrument of attack for criminal or terrorist purposes.

---

[1] "Fostering the Industrial Internet to Accelerate Economic Growth and Transformation," September 13, 2017. Information Technology and Innovation Foundation, https://mail.aol.com/webmail-std/en-us/suite.

[2] "HP Study Reveals 70 Percent of Internet of Things Devices are Vulnerable." http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.VHMpw4uUfVc.

Strategies to Cope with the Internet of Things in the Smart City

The challenge of cyber security keeps getting ever more difficult and the exponential increase in the number of IoT enabled devices makes cybersecurity increasingly difficult. The smart city to deliver on its potential must be able to overcome the difficulties that IoT networking can pose. The IY report on cybersecurity and the Internet of Things explain the problem in the following manner.

> Effective cybersecurity is increasingly complex to deliver. The traditional organizational perimeter is eroding, and existing security defenses are coming under increasing pressure. Point solutions, in particular antivirus software, IDS, IPS, patching and encryption, remain a key control for combatting today's known attacks; however, they become less effective over time as hackers find new ways to circumvent controls.[3]

And in this regard the problems associated with the IoT and the coming IoE may represent one of the most significant problems for cybersecurity in the smart cities of the future.

A Top Smart City Concern: The Internet of Everything and Crippling DDOS Attacks

The advent of malware such as that known as "Mirai" can create a large network of botnet attackers to mount a flood of digital attackers on targeted sites. In particular, this means that the growth of smart devices connected to the web (i.e., IoTs) now allows a cyber attacker to create a massive array of bot-nets to attack a particular web site. The exponential increase in the number of IoT devices that can be used to mount an attack leads to an area of increased vulnerability for any website connected. In the first instances, this type of Distributed Denial of Service (DDOS) attacks against targeted web sites were sufficiently large to crash a site but were modest undertakings. The initial assaults that created the incoming flood of traffic were at a level of several gigabits/second. Today with the Mirai malware a large scale bot-net of unprecedented size can be assembled. Such attacks have now increased to huge dataflows. These attacks can create so-called SYN, GET or POST flood streams. These have now risen from 300 Gigabits/second to over 500 Gigabit/second most recently to even a Terabit/second. These data floods are by created through the assembly of a massive net of bots all accessing a single web site. These data floods are sufficiently large to attack the largest commercial sites or even crash the most sophisticated of national governmental web sites.[4]

---

[3] Cyber Security and the Internet of Things, March 2015 http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf.

[4] Margaret Rouse and Kevin Beaver, "Distributed Denial of Service Attack," TechTarget.com

These DDOS attacks are typically one of the following types:

- **Syn Flood attack** (or Synchronize Flood). The objective is to generate a flood of ACK (acknowledgement) messages. With a SYN flood assault the attacker can easily use fake, random, non-incriminating source addresses for his packets that come from the massive bot-net.
- **GET/Post Flood attack:** This is when an HTTP client (say, a Web browser) talks to an HTTP server (a Web server). In this case the data flood sends requests which can be of several types, the two main being GET and POST. A GET request is what is used for "normal links", including images; such requests are meant to retrieve a static piece of data, the URL pointing to that piece of data. When you enter a URL in the URL bar, a GET is also done. POST requests are used with forms. A POST request includes parameters, which are usually taken from the input fields on the same page. The attacker wants to submerge the target server under a torrent of requests, so as to saturate the server computing resources. Flooding works best when the server allocates a lot of resources in response to a single request. Since POST requests include the need to access parameters within the web site, they usually trigger relatively complex processing on the server (e.g. most database accesses). This involves more processing activity for the server than serving a much simpler GET. Thus, POST-based flooding tends to be more effective than GET-based flooding. It short, it takes fewer requests to drown the server if the requests are POST. On the other hand, GET requests are much more common. Thus, it is much easier for the attacker to enlist (involuntary) help in the flooding effort.[5]

IoT Cybersecurity and the Smart City

The distributed denial of service (DDOS) is of concern to businesses or governmental websites, but fortunately there are defenses against such attacks. This does require precautions to be taken against attacks against Mirai or other similar software marshaling a huge number of Internet of Thing devices in order to convert them into attacking bots. The larger concern is whether IoT systems can be used to attack people, networks, businesses or other specific targets to carry out various types of attacks. These attacks can be quite varied and might include hacking a car so that a driver might lose control, hacking a home security system to find out if

August 2017 http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack.

[5] CharalamposPatrikakis, MichalisMasikos, and Olga Zouraraki, Distributed Denial of Service Attacks - The Internet Protocol Journal - Volume 7, Number 4 https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-30/dos-attacks.html (last accessed August 2017).

anyone is home and then to disable the electronic security system, or carry out any one of thousands of specific hacking-based attacks.

The range of possibilities for hacking that are now possible via the IoT is now a significant worry. A recent report of an attack involved an Internet-based attack on a casino in the United States. This attack involved hackers who managed to use a "smart fishtank" with the latest in Internet of Things (IoTs) technology. In this case the cybersecurity firm Darktrace revealed that the hackers used a fishtank with internet access for the purpose of controlling the temperature, lighting, and filtering of a fishtank's operation to launch a sophisticated cyber assault that probed much deeper into the casino's multi-million dollar operation. After gaining access to the fishtank that was connected to the casino's local area network (LAN) they were then able from this entry point to invade the casino's data base. This unlikely approach shows just how innovative cyber criminals can be. They used a seemingly quite innocent IoT device as the instrument to then link into a casino's data network in order to steal over 10 gigabytes of data and transfer it to a site in Finland. This included among other things the credit card information for thousands of customers.[6]

The U.S. Federal Bureau of Investigation (FBI) has also recently sent out a warning to parents about toys that are connected to the Internet using IoT technology. This alert indicated that hackers might be able to use this means to find out the names and other personal information about children that play with such "connected" toys. These concerns have led to speculation that there might be eventually lead to U.S. governmental regulation and protective standards for products containing IoT connectivity. Currently products in the United States are subject to Federal Trade Commission (FTC) approval, but it is far from clear how IoT products might be regulated and by which agency.[7]

The Internet was first developed by the U. S. Defense Advanced Research Agency (DARPA) as a type of digital network that was of maximum resilience to attack because of the creation of a very large number of interconnected networks. This meant that if a particular network should fail or be disabled due to an attack, another network could still provide connectivity. The military is now seeking ways to use IoT capabilities to further the efficiencies and resilience that comes with this new capability. It is thus ironic that a technology that was invented and now enhanced to increase survivability and resilience has also become an area of cyber concern because of its ability to be attacked in so many different ways.

In order to understand new cybersecurity concerns, it is necessary to understand the both the architecture of the Internet as well as the world wide web that allows the massive transfer of information and content via the global Internet architecture. This ability to transfer data so efficiently is critical to the smart city of the future. This understanding is also critical to the protection of information and the safety of our urban future as well.

---

[6] Alex Schiffer, "Hackers Use Internet-wired Fish Tank to Hook Data" *Washington Post,* July 22, 2017, P. A16.

[7] Ibid.

The Architecture of the Internet and Power of the Internet Protocol

The future of smart cities will be linked for decades to come to the latest version of the Internet Protocol. This is because this protocol provides the essential method and means for linking of all forms of data communication and telecommunications networks in the world today. It is essential for smart city planners as well as urban officials to understand that the Internet is, in fact, a huge number of interconnected and hierarchically arranged networks that links through the world via a variety interface standards, but with the Internet Protocol at its heart.

The packets of information that can travel of the Internet today can be simply data, audio (i.e. voice, voice over IP (VOIP), various qualities of radio), or of course video up to ultra high definition television (UHDTV). The Internet Protocol sets forth the method by which data is packetized, addressed, transmitted, routed, and received. This operation of the Internet and the IP standards that establish the means by which data is organized and transmitted around the world is based on four hierarchical layers. This starts at the lowest known as the link or network interface layer. The link contains the communication methods for data that remains within a single network segment (or link). Next is the Internet layer that provides the rules or protocols for the internetworking between independent networks, so they can be connected. The third layer is the transport layer that establishes the routing or handling of so-called host-to-host communication. Finally, there is the application layer, which provides for data exchange for specific applications.

This four layer systems architecture for relaying packets of data via the Internet is sometimes compared to more complex seven layer architecture that is used in digital telecommunications known as the Open Systems Interconnection (OSI) Model (see Table 10.1).[8]

This OSI model preceded the Internet Protocol (IP) that was also developed to connect a large number of digital networks. One can compare how the much simpler Internet four tiered layer system compares to the OSI model as follows (see Table 10.2).[9]

Essentially this four layer system, with its quite streamlined and compact digital networking interconnection architecture, allows information to be shared from almost any computer platform in the world. Thus global interconnection is possible as long as it can connect to an Internet by wire, cable, wireless, satellite or any other functioning communication system that can support digital networking.[10]

The world of Internet and the world of publicly switched telecommunications are quite different from each other in almost every perspective. The technical standards for the Internet are created through a collaborative process that is undertaken by

[8] The OSI Model's Seven Layers Defined and Functions (April 19, 2017). https://support.microsoft.com/en-us/help/103884/the-osi-model-s-seven-layers-d.

[9] Jack Unger, "OSI and TCP/IP Reference Models" May 16, 2003, http://www.ciscopress.com/articles/article.asp?p=31731&seqNum=2.

[10] Ibid.

Table 10.1 The seven layer open system interconnection reference model first developed for digital telecommunications and the integrated systems digital network (ISDN)

Open systems interconnection (OSI) reference model		
Layer	Protocol data unit	Function of the various layers
7. Application (host layer)	Data	High-level APPs, including resource sharing, remote file access
6. Presentation (host layer)	Data	Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption
5. Session (host layer)	Data	Managing communication sessions, i.e., continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
4. Transport (host layer)	Segment (TCP) Datagram (UDP)	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
3. Network (media layer)	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
2. Data link (media layer)	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
1.Physical (media layer)	Bit	Transmission and reception of raw bit streams over a physical medium

Table 10.2 Comparing the layers in the TCP/IP reference model with the OSI reference model

Comparison of the four layer internet protocol with the seven layer open system interconnection (OSI) model	
Internet protocol	OSI model
Application layer	Application layer
Application layer	Presentation layer
Application layer	Session layer
Transport layer	Transport layer
Internet layer	Network layer
Link layer	Data link layer
Link layer	Physical layer

what is called the Internet Engineering Task Force (IETF). This is group is essentially made up of network designers, vendors of equipment and software, researchers, and network operators. The "mission" of the IETF is to develop, promulgate and promote what are ultimately voluntary Internet standards. These standards comprise what are known as the Internet Protocol suite.[11]

In contrast the world of telecommunications has standards that are developed globally within the overall framework of the International Telecommunication Union (ITU) that is headquartered in Geneva, Switzerland. These ITU telecommunications standards are developed within committees formed largely by experts

[11] Internet Engineering Task Force (IETF). http://www.ietf.org/.

from telecommunications organizations around the world and these standards are developed for wire, cable, and fiber-optic networks on one hand and for wireless and satellite systems on the other. In a number of cases special arrangements need to be established or standards adjusted to make the interface standards for wire-based systems and wireless networks. The telecommunications world is oriented toward interconnection and interface standards based on the seven-layer OSI reference model while the IT networking world is based on the four-layer TCP/IP reference model. These two systems are in many ways incompatible and this not only involves these seamless interconnections, but also involves issues with security and issues with routing headers, virtual private network security, seamless interconnection between telecommunications networks and IT networking via Local Area Networks (LANs), Metropolitan Area Networks (MANs) and World Area Networks (WANs).

As long as there are two different standards-making hierarchies for telecommunications and IT networking this going to remain a problem with seamless interconnection and especially problems related to systems security. Adding on top of this the greater complexity as to how many IoT devices that are accessing the Internet on a global basis, the problem is only going to become more difficult security issues more complex and harder to solve. In short one of the key compatibility and security issues to be addressed is that the networking world (Internet and the IETF) and the telecommunications world (the telecom operators and the ITU standards processes) are independent of each other and do not also have the same approach to operating and making secure digital transmission of what should be protected information.

Emerging IoT Applications: New Solutions and New Problems

The Internet of Things (IoT) as it evolves into the Internet of Everything (IoE) will pose new challenges to cybersecurity, but on the other hand also offer new opportunities. It will indeed be a "two-edged sword" that can cut in both a positive and negative direction. Ironically the new applications can offer new types of security yet in the wrong hands will create security or other forms of social, economic or political problems.

Geofencing and Global Satellite Connectivity: Opportunity and Potential for Abuse

One area where IoT devices can assist with security in the "smart cities" of the future is a new concept that is known as 'geofencing' which is a newly coined term to describe a new form of electronic security. This is the idea of creating a global network for corporations or organization with a large number of assets deployed around the world with every asset connected to an IoT device that constantly updates

a global data base as to its exact location using Global Navigational Satellite Services (GNSS)—typically GPS services—to indicate that the asset remains within an area that is defined within a "geofenced" limited location. Although many of these security networks might use terrestrial wire or wireless networks, global asset management will likely make use of satellite to create a comprehensive map of all there "mapped resources" on a world-wide basis.

As Julia McGowan of Globecomm has stated on this subject: "IoT offers industrial companies new and better options for protecting assets than in the past. Among the most powerful is geofencing: the ability to track the location of valuable assets and establish a virtual "fence" around where they are supposed to be."[12]

The objective of many worldwide enterprise networks is to be able to devise a networking and data management systems that is integrated so that it can operate off of a single platform. The ideal scenario for a truly global enterprise, according to strategic analysis stated by Globecomm would be for a company or organization operating large (i.e., gigabyte) data flows would be to have "one platform for everything, including: provisioning, billing, invoicing, and network management, with the outcome being more streamlined operations." This network, for security reasons, however, would have to have complete backup capabilities and this would require immediate access to an entirely independent and separate geographic location. Such a system would therefore likely need to be satellite-based in order to have true global coverage and to have independently located back-up systems.[13]

The applications for inventory control and other uses such as keeping people away from harmful locations are numerous. Yet, as is the case with most technologies, a new capability can give rise to difficulties or harmful uses. A cybercriminal that hacks into such a data base might use the "geofencing" information to target thefts or hide embezzlement. A techno-terrorist could use such information to locate weapons, seek out radioactive materials, or for other heinous purposes. In the case of a time where embedding of chips in people becomes commonplace, IoT-enabled devices might be used to track political opponents or create a totalitarian regime with enormous powers of control. Efficient and seemingly innocuous technology could lead in time to a future Brave New World. Such technology clearly will need effective controls and harsh penalties for misuse.

Standards, Regulations, or Legal Prohibitions to Assist in Preventing Misuse of IoT/IoE

Once a technology or a digital application is developed and proves useful, it is really not possible to "uninvent" it or is widespread use. The Internet, smart phones, digital networking, fiber optics, broad band wireless and satellites are here to stay as are the Internet of Things (IoT) and soon the Internet of Everything (IoE). The

[12] Julia McGowan, "The Internet of Things Is Out of this World – A Globecomm Perspective" *Sat Magazine*, September 2017 http://www.satmagazine.com/story.php?number=412528056.

[13] Ibid.

challenge in the age of smart cities, smart buildings, smart infrastructure, smart vehicles, and more is not to prohibit the use of new technology and new applications, but rather to create technical standards or design processes that help to prevent abuses or to create regulations and laws that can be enforced to prevent misuse of these new capabilities. Table 10.3 sets forth a number of possible uses and abuses

Table 10.3 Concerns with Internet of Everything (IoT) security and possible remedies

Uses and abuses of IoT-equipped devices and possible standards or regulatory remedies			
IoT/IoE application	Abuse	Technical standard	Regulatory action
Geo-fence monitoring of IoT-devices for inventory or physical security access control	Identification of materials for theft or sabotage of infrastructure	High level encryption	"Invasion" of "geo-fence" considered a global felony with additional penalty if theft involves radio-active materials
Security camera system for home, industrial or government site	Surveillance to know when to attack a site	High-level encryption	Define such abuses as a felony
Driverless car devices	Disable vehicle or cause it to crash	High-level encryption	Define such abuses as a felony including possible charges of manslaughter or murder if there is loss of life
Electrical power grid monitor and switches	Disable or assault on power systems	High-level encryption	Define such abuses as a felony including possible charges of manslaughter or even murder if there is loss of life
Building elevator or escalator operations	Disable or assault on elevators or escalator systems	High-level encryption	Define such abuses as a felony including possible charges of manslaughter or murder if there is loss of life
Water, sewage or gas supply or distribution system operations	Disable or attack on such a utility	High-level encryption	Define such abuses as a felony including possible charges of manslaughter or murder if there is loss of life
Transportation systems operations (rail, metro, airport, traffic signals)	Disable or other forms of attack	High-level encryption	Define such abuses as a felony including possible charges of manslaughter or murder if there is loss of life
Operation of any form of infrastructure, security system, transport or service on which people depend such as bldg. HVAC, etc.	Disable or other forms of attack	Encryption or reasonable level of code word access	Define such abuses as a felony including possible charges of manslaughter or murder if there is loss of life

for IoT-enabled devices and protective standards, regulations or legal provisions that might be devised relative to these applications.

The able examples are on illustrative, but the key is that such attacks should be considered quite serious attacks and defined explicitly as felonies with significantly heavy penalties. Hacking into protected systems, especially those on which peoples' lives depend should be considered an attack on society and explicitly defined as a most serious crime. One of the key legal issues is that many such attacks are made across international borders. This means that international treaties need to be adopted to define these crimes on a global scale and that harsh penalties are internationally agreed on and enforced across international boundaries.

Conclusions

One of the basic building blocks that will constitute the 'intelligence' in the 'smart city' will come via the Internet with the overwhelming amount of that information being originated from many billions of IOT-enabled devices. The exponential growth of Internet of Things (IoTs) devices across the world and into every aspect of life—including IoT chips now being embedded into people and medical implants—represents a watershed in terms of how the Internet now impacts most peoples' lives. This is now not only on a daily but minute-by-minute and even second-to-second basis. The loss of functionality of an IoT-enabled device can affect vital operations of infrastructure in ways that can involve actual survival, just as a gun or knife or hand grenade is defined as a weapon, we have now come to a point where an IoT-enabled device has also become not only a weapon, but even a weapon of mass destruction.

This vital transition makes it essential that appropriate safety and technical standards be developed and approved—on a global basis—to help protect lives. There will be a growing number of safety and technical standards to help ensure the appropriate use and operation of IoT-devices. Almost every aspect of a 'smart city' operations will be affected. Therefore, there is a need for criminal legislation to define Internet-enabled crimes. In a more secure world for 'smart cities' penalties for abuse will be enacted all levels of government. There is an urgent need for the adoption of a global treaty to ensure that hackers, cybercriminals, and techno-terrorists around the world clearly recognize that they are going to be found, charged, prosecuted and sent to jail—or worse. Cyber-attacks are now truly serious crimes with very significant consequences. Protective systems against abuses of the coming Internet of Everything is urgently needed to reap the extraordinary benefits of 'smart cities'.

Chapter 11
Coping with the Dark Web, Cyber-Criminals and Techno-Terrorists in a Smart City

The focus of this chapter is on efforts to curtail the activities of cyber-criminals and the latest strategies as to how this might be accomplished. This includes addressing efforts to identify, catch and prosecute cyber-criminals, methods to identify them, and the tools available to them via such mechanisms as the dark web. We also explore the latest protective strategies that can be used to secure vital sites against cyber-attacks. The world of the Internet and the continuing global spread of cyber-services and new capabilities such as the Internet of Things, the cloud, and industrial control systems such as SCADA networks has expanded the scope of cyber-crime and redefined the scope of security systems in the smart city.

In days of old, when one wanted to seek help in carrying out a nefarious deed or engage in a criminal act and needed help, the likely approach would be to go to the seediest bar on the waterfront and start asking around for a likely ex-convict from prison to help out in the misadventure. Today, in the world of Internet, the process is dramatically different. The key might well be to find out a means to access the so-called dark web, where identities are protected and the tools of the trade associated with cybercriminal activities are up for sale. Everything is anonymous today as the covert electronic currencies such as ZCash crypto-currency and bitcoin flow freely around the world. Here one can buy stolen credit card numbers, e-mail addresses, stolen medical records, or the latest in ransomware, Trojans, data bombs, and various types of malware. It is like a one-stop shopping mall for planning criminal operations.

The terminology that is used with regard to the dark web—overlay networks, the dark net and the deep web—is sometimes a bit confusing. These terms are defined in the book's glossary. The main thing to be clear about is the difference between the deep web and the dark web. The deep web refers to the part of the Internet that, for a variety of reasons, is not accessible by search engines. This can be as much as 90% of the content of the Internet, and many of these functions are related to the actual operation of the web and have nothing to do with criminal activities. The dark web is the part of the web where the identities of those accessing it are hidden, often because they are engaged in nefarious or criminal activities. Others, such as journalists or cybersecurity experts, might access it for research purposes.

© Springer International Publishing AG, part of Springer Nature 2019

J. N. Pelton, I. B. Singh, *Smart Cities of Today and Tomorrow*,
https://doi.org/10.1007/978-3-319-95822-4_11

To access these hidden networks or encrypted networks typically requires specialized software. The conventional web that is accessible to search engines is often referred to as the clearnet, since these sites on the worldwide web are not encrypted. Secure sites that are identified as https that are protected but not encrypted against search engines are still considered a part of the clearnet. Tor, Freenet and I2P are the most commonly used encrypted networks that are in use by those operating within the dark web.

The spread of cyber-criminal behavior is increasing. People might undertake cyber-crime for a variety of purposes, ranging from minor to the most serious felonies. These include simple hacking operations, often by young people, who might want to change a grade, carry out some form of surveillance, pull a prank on someone or find out embarrassing secrets. Hacking could even be simply to show one's computer prowess in penetrating a secure site. All of these activities are still criminal acts and are subject to legal prosecution.

There are other types of cyber-criminals who are motivated by greed. The objective of these types of cyber-criminals is to steal money from banks or ATM machines, or steal credit card information, or they may use ransomware to blackmail people into paying to get back on their computers from which they find themselves locked out by intrusive malware.

Others can use the dark web for even more serious felonies. The dark web, for instance, has been used to recruit murderers for hire, those willing to engage in armed robbery, extortion, or other violent crimes. Unfortunately crypto-currencies have also been used to undertake or support criminal activities such as money laundering and for hiding kidnapping payments.

The first subject to address in greater depth in this chapter is that of the dark web. This is because it is a prime source of growth of cyber-criminal activities and represents a key challenge to law enforcement that demands serious attention.

Strategies for Coping with the Dark Web

The dark web, also called overlay networks, uses the Internet but requires specific software, configurations or authorization to access. This is in order to ensure that they are blind to search engines. The dark web represents just a tiny part of what is called the deep web. In the case of the dark web or dark net, identities are specifically hidden because these users are up to no good. However, this is not exclusively the case. Sometimes law enforcement officials or reporters might use the dark web to undertake research or ensnare cyber-criminals. On the other hand the deep web represents a very significant part of the software operating within the Internet, and these activities are critical to the Internet's smooth international functioning and synchronization. The intentionally hidden dark net represents a very small amount of the Internet software activity—perhaps under 0.01% of the total activity.[1]

[1] Solomon, Jane (6 May 2015). "The Deep Web vs. The dark web". https://law.ku.edu/sites/law.

Table 11.1 The expanding use of the dark web (courtesy of the Rand Corporation)

Key trends involving the dark web from the Rand Corporation Report
1. The hacking community and cyber black markets are growing and maturing
2. The cyber black market has evolved from a varied landscape of discrete, ad hoc individuals into a network of highly organized groups, often connected with traditional crime groups (e.g., drug cartels, mafias, terrorist cells and even nation-states)
3. The cyber black market does not differ much from a traditional market or other typical criminal enterprises; participants communicate through various channels, place their orders and get products
4. The evolution of the black market within the dark web mirrors the normal evolution of markets with both innovation and growth
5. The cyber black market can be more profitable than the illegal drug trade
6. Cyber black markets respond to outside forces
7. Because of an increase in recent takedowns, more transactions have been moving to the dark net; stronger vetting is now taking place; and greater encryption, obfuscation and "anonymization" techniques are being employed, restricting access to the most sophisticated parts of the black market
8. The proliferation of "as-a-service" and "point-and-click" interfaces lowers the cost to enter the cyber black market
9. Law enforcement efforts are improving as more individuals are technologically savvy; suspects are going after bigger targets and thus are attracting more attention; and more crimes involve a digital component, giving law enforcement more opportunities to catch crime in cyberspace
10. Still, the cyber black market remains resilient and is growing at an accelerated pace, continually getting more creative and innovative as defenses get stronger, law enforcement gets more sophisticated, and new exploitable technologies and connections appear in the world
11. Products can be highly customized, and players tend to be extremely specialized

Dark net sites come in many shapes and sizes. These can be quite small and specialized in the form of friend-to-friend or peer-to-peer network or they can be quite large networks such as TOR, Freenet, and I2P (which stands for Invisible Internet Project). In short, dark nets can be, operated by individuals, criminal syndicates, terrorists groups, law enforcement groups, or private or public organizations. Users of the dark web sometimes refer to the regular web as the clearnet, since most of the Internet is searchable by search engines and is not encrypted.

A key report from the Rand Corporation on the operation and expansion of the criminal and terrorist aspects of the dark web provides a useful overview of trends with regard to its use. Its 11 key findings that summarize the full report are provided in Table 11.1[2]:

Another term that is often used with regard to criminal uses of the dark web is the Silk Road. This name became notorious for several years when it was used to iden-

ku.edu/files/docs/media_law/2017/panel-3-annotated-bibliography.pdf Retrieved August 16, 2017.

[2] Lillian Ablon, Martin C. Libicki, Andrea A. Golay, "Markets for Cybercrime Tools and Stolen Data: The Hackers' Bazaar" Rand Corporation Report, http://www.rand.org/pubs/research_reports/RR610.html (2014).

tify one of the largest and most notorious of the sites on the dark web. This site (under the name Silk Road 1.0 and Silk Road 2.0) was operated by a cybercriminal named Ross Ulbright. He was eventually arrested, prosecuted and went to jail. The Silk Road that is now operational on the dark web is now known as Silk Road 3.1 and is, in fact, a whole new operation no longer associated with Ross Ulbright. The history of Ulbright's arrest, the legal arguments as to why he was considered legally culpable and could be sent to jail is discussed later in this chapter.

The Current Status of the Dark Web

Today cybercrime conducted by means of the dark web can be highly profitable, is more difficult to detect and successfully prosecuted than conventional crime, and in some cases not even brought to light until a significant amount of time has passed. This creates a significant incentive for computer savvy people from around the world to be drawn into cybercrime. Even those that might initially seek to learn about the dark web for purposes of law enforcement or counter terrorism vigilance might be tempted in time to abuse their learned skills by engaging in illegal cybercriminal activities once they become proficient in accessing the dark web.

Today there are plenty of resources to go to learn how to access the dark web. There is the Dark Web Newsletter (https://darkwebnews.com/), Anonymity Newsletter (techcrunch.com/2015/02/14/the-anonymity-network-at-risk) and many more.

On the Deep Web Newsletter website, they claim to have cataloged a list of some 7839 Deep Web Links in an uncensored table. They also claim to have checked out each of these links so as to categorize them, record the name of the site, give a description of the site, record if it was online or offline or dead, what they sell and even provide screen shots.[3]

Personal Anonymity on the Internet

Before examining the dark web in great depth it is perhaps most useful to examine how one might, for legitimate reasons, wish to protect one's anonymity and patterns of usage on the Internet. In March 2017, the U. S. Congress agreed to new legislation that President Trump signed into law that allowed Internet Service Providers (ISPs) to sell information about their users' patterns of use on the web. In particular, this means that Verizon, Comcast, AT&T or others, in addition to browser services, to track and share people's browsing and app activity without permission This new legislation reversed restrictive regulations created by the FCC during the Obama

[3] 7839 Awesome Deep Web Links List [Uncensored Table] August 15, 2017 https://darkwebnews.com/deep-web-links/.

administration in order to prevent ISPs from selling information about how their customers use the Internet.[4]

Mignon Clyburn, the FCC commissioner claimed that the FCC regulations that were overturned by the Congressional Review Act of 2017 would adversely impact user privacy. She said: "The [FCC] rules gave individuals control over their information when it comes to privacy. The proprietary information these companies have at their disposal should not only be treated with care, but consumers should have a voice."[5]

Thus Internet users who wish to protect themselves against cyber-criminals as well as intrusions into their privacy by ISPs and browser search engines have no real choice except to hide their IP addresses. Fortunately in Canada and some parts of Europe there remain protections, but it is not clear how long these protections will remain. In response to terrorism attacks that have been carried out in Germany, France and the U. K. there have been new legislative and executive actions carried out to prevent the use of social sites such as "Viber" and "WhatsApp" to hide one's identity and personal privacy in messaging.

If one's IP address is effectively hidden it can help protect your digital footprint, bypass any content filters or blacklisting, prevent any web tracking and hide your geographic location and identity**.** This effort to achieve Internet anonymity can help protect one against hackers, stalkers or simply unwanted spam.[6]

Four Ways to Hide Your IP Address

There are four primary ways to hide one's IP Address and these are to: (1) utilize a Virtual Private Network (VPN) service, (2) employ TOR (The Onion Router) encryption, (3) access the web via a proxy server, or (4) use a free/public Wi-Fi service.

1. *VPN Server:* Using a VPN service is considered by many to be the best way to hide one's IP address. If you are enrolled with a VPN service then when you go online you will display a different IP address that you will be "loaned" each time you go online that the service automatically provides. One can sign up with any one of these VPN services. When you go online, you will be showing the world a different IP address. This is one that will be "loaned" from the service you're using.
   Some of the advantages associated with using a personal VPN service over a proxy service include the following: high speed bandwidth, more versatile usability, a secure connection, private access to blocked sites, and the ability to choose the country and city where you appear to be originating from on a global

[4] Cecilia Kang, "Congress votes to overturn Obama era online privacy rules" *New York Times*, Technology, March 28, 2017. https://www.nytimes.com/2017/03/28/technology/congress-votes-to-overturn-obama-era-online-privacy-rules.html?_r=0.

[5] Ibid.

[6] How to Hide Your IP Address (August 15, 2017) http://whatismyipaddress.com/.

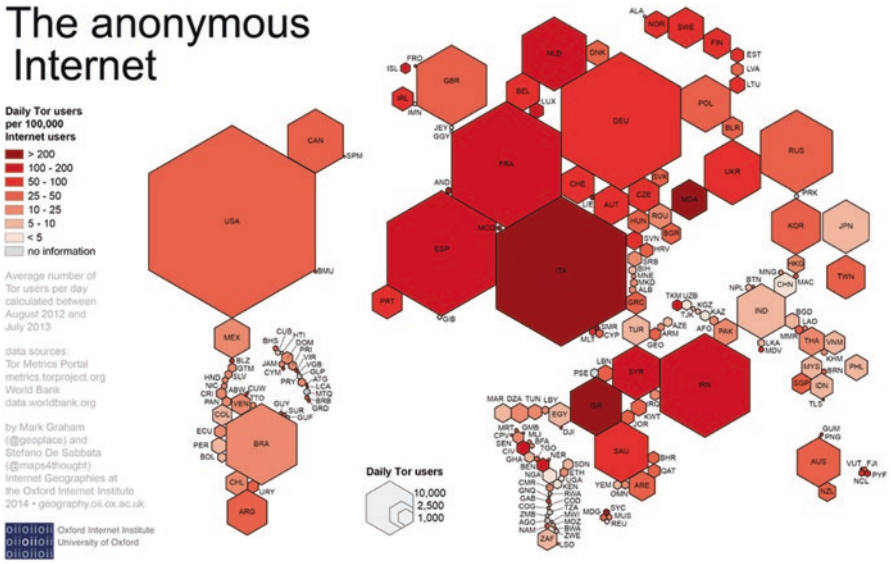

Fig. 11.1 A cartogram showing national usage and density of TOR globally (courtesy of Mark Graham, Oxford Internet Institute, University of Oxford)

basis. Further there are many hundreds of VPN services that you can sign up with on a worldwide basis. Unfortunately they vary widely in quality and reliability. Some of the better known and reliable include: ExpressVPN, IP Vanish, Cyber Ghost VPN, NordVPN, Hide.me VPN, and SaferVPN. These services will connect to a range of 25 to over 190 countries.

2. *TOR:* The Onion Router (TOR) is free software that represents a second generation of what is known as onion routing. This encryption-based approach can allow Internet users to communicate anonymously over the Internet. There are problems with this approach in that traffic analysis techniques can be used to match an IP user with a specific point of origin. It is also the slowest option because the encryption slows your access to the Internet. By matching patterns of use, law enforcement cybersecurity officials use TOR tracking over time to link someone to a particular IP address. The second generation of encryption software associated with TOR, however, now makes this quite difficult to do. This approach is less effective than a VPN service but is also free.

   Anyone from anyplace in the world with Internet service can use TOR to search the web and communicate with others. As noted above this process is free and the key is that the data services that flow onto and from the web comes in the form of a layered heavy-duty encryption that ensures security and privacy protection. The TOR browser (like Chrome, Firefox or Safari) is a free software program that can be downloaded onto a computer in order to conceal a personal IP address every time that an individual goes online. This process allows one to become anonymous when the Internet is accessed. (Figure 11.1 presents a cartogram mapping of TOR usage on a global basis as of 2014, showing the level of usage

as well as density of use on a country by country basis as presented by Oxford Internet Institute, Oxford University.) It is interesting to note that the largest number of TOR users is in the United States, but the highest density of use is in Italy, Israel, and Moldovia.

3. *Employing a Proxy Server:* A proxy server can be used to re-route your browser. This can be done to go around company or school content or in the case of some countries national restrictive filters. There are possible downsides that can come from seeking to "mask" one's IP address by use of a proxy server. Most proxies will slow down your Internet connection. In some cases proxies can involve compromised machines. Perhaps most serious the use of proxies may not be legal in some countries with restrictive access to the web, and this can involve criminal charges.
4. *Use Free/Public Wi-Fi:* If you can also use a free or at least public Wi-Fi then the IP address you will be using will not be your own. You can go to a library, bookstore, mall or coffee shop and sign on to the Internet with its IP address. To verify this is the case one can go to "WhatIsMyIPAddress.com" and to check what IP address appears when you log on from your personal computer. Next go to a public Wi-Fi and then log into the Internet from a Wi-Fi hot spot. One can then go back to WhatIsMyIPAddress.com and check it again. This will confirm that you are identified with the Wi-Fi's IP address and not your own unique IP address. However, this approach has a definite risk. If you don't use a VPN, your Internet activity is at risk of being intercepted by anyone with a scanner. There are many employees that are telecommuting from home that use a wireless router in their home that will log into a corporate confidential system without realizing they are exposing confidential information to someone nearby with a scanner. Wireless routers, public Wi-Fi systems and the like are easily compromised. Particularly do not check your bank accounts, brokerage account, or corporate files using a public Wi-Fi hot spot or even a wireless router in your office or home.

Prosecuting Operators of Dark Nets Engaged in Criminal Activities

The legal basis on which cyber-criminals operate on the dark net is still being developed in the United States and other countries that are seeking to curtail such operations. One of the most important cases involves the operation of the so-called Silk Road.

In 2013 Ross Ulbricht, also known as the Dread Pirate Roberts, then 28 years of age, was arrested for his alleged operation of the Silk Road. He was formally indicted for narcotics trafficking, computer hacking, money laundering, conspiracy to traffic fraudulent IDs and engaging in continuing criminal enterprise. He pled not guilty on all charges in January 2015, but was convicted in February 2015 of money laundering, computer hacking, conspiracy to traffic fraudulent identity documents,

and conspiracy to traffic narcotics. He was sentenced for operating the billion-dollar Silk Road dark net to a life sentence without parole. In 2017 his conviction and sentence was upheld by the U. S. Court of Appeals for the Second Circuit.

There was originally a Silk Road 1.0 and 2.0 started by Ulbricht and perhaps other conspirators. This has now morphed into Silk Road 3.0 and Silk Road 3.1 that is carrying on dark web clandestine operations. This most notorious of the known criminal dark net sites under its current 3.1 nomenclature is purportedly being widely used to buy and sell drugs. There are thought to be other illegal activities conducted on this dark net site that includes money laundering, selling of stolen credit card numbers and perhaps even murder for hire. The conviction and sentencing of Ulbricht are keys for setting a legal precedent. Based on this trial and conviction of Ulbrecht, it has been established that operators of dark net sites for proven criminal purposes can be considered to be equivalent to engaging in these same criminal activities as conducted elsewhere.

The defense attorneys for Ulbricht sought to use a constitutional defense by invoking the Fourth Amendment that protects personal privacy. This amendment protects every U. S. citizen's right to be free from unreasonable government intrusion into their persons, homes, businesses, and property. This constitutional right was judged not to extend so far as to be considered a reasonable defense against the right to operate a clandestine dark net site for the purposes of engaging in criminal enterprise. The future of how to protect one's privacy whether for legitimate, criminal or even terrorist purposes is uncertain. There are those that will attempt this by means of encrypted Internet-based privacy or other ways to hide one's financial activity via electronically encrypted means such as bitcoin. There are, of course, data havens such as Bermuda, the Cayman Islands, the Netherlands, Switzerland, Singapore, Ireland, Luxembourg, Curaçao, Hong Kong, Cyprus, Bahamas, Jersey, Barbados, Mauritius and the British Virgin Islands that are now used to hide income from taxation or forms of money laundering.[7] And now there are even thoughts of creating data havens in space such as the stated purpose of the Asgardia 1 launch of a cubesat that has stored and secured messages submitted to it from individuals all over the world prior to the launch. In this case there are many questions about how data could be retrieved and what happens when the cubesat's orbit deteriorates and the cubesat falls back to Earth. In time, however, secure and encrypted data on which the public, corporations can very likely be stored for very long periods in space.[8]

[7] Nassim Khadem, "Bermuda tops list of world's top tax havens according to Oxfam" Sydney Daily Herald, December 12, 2016. http://www.smh.com.au/business/the-economy/bermuda-tops-list-of-worlds-top-tax-havens-according-to-oxfam-20161208-gt6v3n.html.

[8] "Asgardia's 1st satellite due to launch" Earth Sky, June 28, 2017 http://earthsky.org/space/asgardia-space-nation-satellite-launch-2017.

Protecting Smart Cities from Criminal Cyber Activity

One of the true concerns about the future of smart cities is how to protect them from criminal activity as well as terrorist attack. These of course can be carried out with collusion between criminals and terrorists, but for this discussion the two types of activities will be separated. Criminal cyber activities are directed at obtaining some form of financial gain, while terrorist attacks are directed at inflicting various types of pain on real or perceived enemies. Thus cyber-terrorists can attack infrastructure, transportation or energy systems, farms, water and food supplies, medical systems and supplies, banking systems, or any electronic or IT system on which the public, corporations or governments rely on to survive, operate or sustain a population. In short, criminal cyber-activities are much more narrowly directed and easier to detect and characterize on one hand, but are also more prevalent and pervasive on the other.

The cyber-criminal activities that are of prime concern and for which it is important to find ways to eliminate or greatly reduce them in the smart city of the future include the following big three. These top cyber crimes include: (a) obtaining of stolen credit cards through the hacking of personal computers or smart phones or purchasing them off of the dark web after high-level hackers steal tens of thousands if not millions of cards off of a large corporate site or banking system. (Credit card fraud is perhaps the most prevalent of cyber-crimes and most persistent. The new chip-based EMVcards help but are not a silver bullet solution to this problem); (b) hacking of banking systems or corporations with high-level financial accounts using Trojans or other means to either steal money electronically or to extort money to receive back stolen account information; (c) use of ransomware to extort money so that users can regain access to their computers from which they have been denied access until they pay a ransom. Unfortunately new ways to use cyber-techniques to acquire money illegally will continue to grow and expand both in nature and in geographic area as more people use the Internet.

And sometimes the nature of these attacks is not immediately obvious, and the stopping of a malware's spread involves unconventional means. The world's largest ransomware cyber-attack, which occurred in May 2017, is a case in point. In this instance there was a truly massive cyber-attack with the victims being spread across a reported 99 countries. Even hospitals and medical centers had their computer systems shut down in the United Kingdom, train schedules were disabled in Germany, and the largest computer assaults were reported across Russian in this worldwide attack. Despite the demanded $300 ransom to restore service, it was not clear how many paid this ransom. Some experts have even suggested that this could have been a dress rehearsal for a future terrorist attack.[9]

The key to this attack was the so-called Wanna Decryptor 2.0, and it was enabled by the leak of information from a U. S. National Security Agency (NSA)-encrypted website that had detected a significant vulnerability in Microsoft software. This

[9] Elizabeth Dwoskin Karla Adam et al., "Nations race to contain hacks" Washington Post, May 14, 2017, P A1 and A7.

weakness was exploited for the attack and involved the rapid spread of this malware. In this case a 22-year-old who tweets under the name @MalwareTechBlog quickly registered a website that ended in "gwea.com" that allowed a kill switch to be activated in the malware that allowed the spread of this cyber-attack to be slowed and eventually stopped.[10]

The predominate approach to deal with most cybercrime is essentially defensive in terms of creating complex cyber access codes, creating firewalls, and creating protective systems to prevent unwarranted use of large databases such as for credit card files. The true route forward to better protection to websites and encrypted access to the Internet via individual smart phones or personal computers seems to call for an offensive rather than simply a defensive strategy. This is, of course, an ongoing battle. The latest smart phones are now using facial recognition unique to a particular user rather than an access code. Perhaps a similar logic system embedded in a smart card or reader system could be geared to a particular biometric unique to an individual.

Already there are employees of some corporations that have a unique embedded chip that allows them entry into protected sites and to purchase products. One might envision a future world where a chip or biometric that does not change with age is used as a personal identifier and for all financial, credit, passport, voting, and legal transactions from birth to death. Such an approach to the smart city would raise all types of questions with regard to personal privacy. Clearly there would be a strong potential for abuse in terms of political control within a totalitarian society. In order to suppress cyber-crime and credit card abuse with such technology, there could well be the possibility of political abuses and suppression of liberty and freedom.

Combatting Techno-Terrorism and Cyber-Attacks on Nations

As noted earlier, the use of cyber-attacks for terrorism purposes is largely different from a cyber-criminal assault. This is because havoc can be created in some many different ways in a technologically sophisticated society. In the future, with the advent of smart cities, the potential only increases. This suggests that there must be a mostly failsafe means to protect automated systems and networks, infrastructure or facilities that are controlled by automated networks, heuristic algorithms or artificial intelligence that might be attacked by cyber-terrorists. This means that ultimately these systems must somehow be programmed so as to not allow destructive or malicious behavior and to stop and shut down rather than initiating activity that could result in harmful results such as death or injury to humans. Not too ironically this suggests something closely akin to Isaac Asimov's three laws that were expressed in the science fiction novel *I Robot*. These now famous three laws stated:

[10] Rick Noack "How a $10.69 purchase may have sidelined the global malware attack" *Washington Post*, May 14, 2017, p. A7.

> "A robot may not injure a human being or, through inaction, allow a human being to come to harm.
>
> A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.
>
> A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws."[11]

The ability to create software sufficiently self-aware so as to recognize that a change to that software would be injurious or potentially lethal to humans is, of course, many years away from potential implementation. In the interim there must be protection against unauthorized access to systems that control the operation of potentially deadly industrial or infrastructure controls. As noted in the previous chapters this a substantial list of things to be protected such as SCADA automated controls for water and sewage, traffic control signals, elevators, train track switches, heating, ventilating and air conditioning systems for buildings and facilities of all types, power plants—including nuclear power plants—telecommunications and IT networking systems, etc.

Today there are millions of SCADA controls at work around the world. In the age of the Internet of Things and the coming age of the Internet of Everything the ability to do harm by remote control via distributed denial of service (DDS), via switching off of security monitoring, and a myriad of other factors increases exponentially. The level of protection against terrorist cyber-attacks must thus also increase to provide protection against spurious commands, malware being installed within automated systems and much more. When there is an attack against various automated systems there must be a system for not only reporting the cyber encroachment and how the attack was stymied but a triggered response to look for parallel attacks elsewhere. This must be the case, whether the attack was against telecommunication switches, water purification systems, traffic signals, oil refineries, stock exchanges, or train switches, etc.

The research firm IDC has attempted to create a cumulative tabulation of what companies, governments and other organizations spend each year on cybersecurity activities. Their estimate for 2016 came to $73 billion for all such activities. This figure will only increase in coming years. This activity includes all such efforts to combat cyber-crime, cyber-terrorism and other attempts to protect personal privacy, and it will undoubtedly continue to increase. The efforts to not only protect online privacy and thwart cyber-attacks going forward will need to go beyond sealing off databases from attacks and create a systematic way to diagnose attacks and combat similar or parallel attacks going forward.[12]

The U. S. National Institute of Standards and Technology has developed the first step in this direction by creating a six-step process for identifying attacks, protecting

---

[11] Asimov, Isaac (1950). *I, Robot* (The Isaac Asimov Collection ed.). New York City: Doubleday. p. 40. ISBN 0-385-42,304-7.

[12] Op cit, Eliabeth Dwoskin, p. A7.

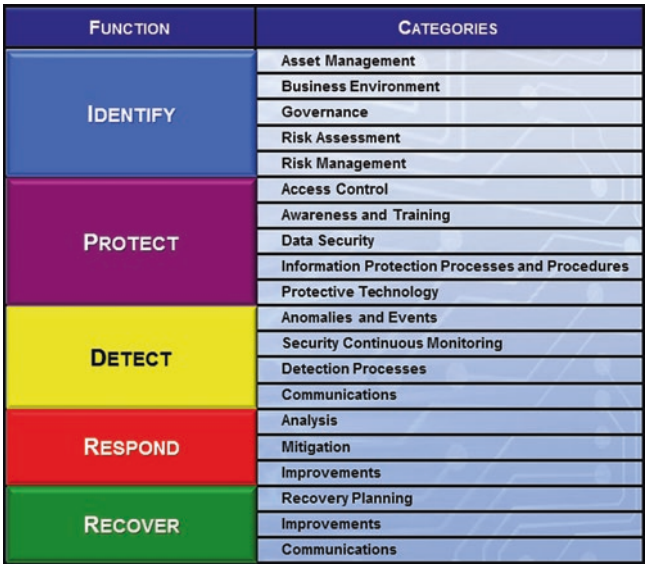

Fig. 11.2 The U. S. cybersecurity framework as developed by NIST (Graphic courtesy of Planet Defense LLC)

assets from attack, detecting the nature of such attacks, formulating a systematic response, and speeding recovery (see Fig. 11.2). This, however, is only the first step in developing a proactive way to respond to attacks in such a manner that future attacks can be mitigated and perhaps prevented. The key is not to just prevent an attack at a particular location or database but to create a process to prevent similar attacks elsewhere and to detect the attacker and so that all future attacks are negated.[13]

Conclusions

The threat posed by cyber criminals continues to grow for many reasons. The tools to engage in cyber-criminal behavior are more and more available, particularly via the dark web. There are a number of countries that almost see cyber-criminal behavior as a local growth industry, and as long as these activities are directed outside their borders they are not particularly vigilant in policing these efforts nor willing to grant extradition for suspected offenders. There are those who do not necessarily engage in cyber-related offenses who can nevertheless benefit from these crimes through the purchase of medical records, social security numbers, credit card information, or other illicitly obtained information off the web or via scanners or other

[13] Cyber Security: Defending SCADA and Industrial Control Systems, Los Alamos Technical Associates, White Paper No. 2, Global Institute for Security and Training, 2014, p. 12.

devices that can obtain information illegally by electronic means. There are now other enabling systems that can support criminal behavior such as crypto-currencies, data havens and more.

The dangers that society is exposed to in today's electronic age simply keep growing as we as a global society become more enmeshed in a cyber-world. The perils that come from living in this new cyber ecosystem vary enormously. Some people act as "trolls" on the web. In this way they can spread embarrassing, malicious and even financially ruinous, racist, or otherwise very damming information about people. This information may, or may not, be true and may well be illegally obtained. Some people do not consider trolling a crime, but a sizable number of young people have committed suicide as a consequence of evil trolling. Many trolls are extremists, racists or at best social misfits. The range of cyber-crimes continues on from trolling to scamming, larceny, corporate fraud, electronic bank robbery, money-laundering, embezzlement, framing someone for a crime, including murder, and even advertising for murder for hire.

Today national and international criminal investigation organizations such as the F.B.I., Interpol, and others coordinate their efforts to combat cyber-criminal activities, but this is clearly insufficient. What is needed is a binding treaty that all nations in the world would sign. Such a treaty would define a wide range of cyber-crimes, agree to extradition for cyber-criminal offenders to stand trial, establish worldwide standards of punishment for these crimes, and also place limits on data havens and crypto-currencies. Today aspirations for such a universal treaty remain a pipe dream. Instead there must be stronger national laws that define a wide range of cyber-criminal activities. There needs to be increased coordination among as many police agencies as possible around the world. There needs to be tougher sentencing—particularly for repeat offenders. Rogue states that harbor cyber-criminals should even be subject to stiff sanctions.

Finally educational programs should be significantly increased to provide better cybersecurity training. Students and the general public need to be trained as to reasonable cybersecurity practices. There also needs to be stricter security standards and systems devised for cell phones, tablets, computers and all electronic devices. This, of course, leaves hanging the ongoing debate about personal electronic privacy and encryption systems such as Pretty Good Privacy (PGP) and the mission of agencies such as the National Security Agency (NSA) and its effort to monitor use of telephones and the Internet to uncover the plotting of techno-terrorists. This issue is addressed in the following chapter.

Chapter 12
How Nations and Smart Cities Can Cope with Cyber-Terrorism and Warfare

The previous chapter largely addressed the issue of cyber-crime and the dark web. At the end of this chapter it began to address the even more serious issue of cyber warfare and the need to find ways to combat techno-terrorism without violating citizens' rights to privacy. This is a thorny issue where some compromise on both sides might ultimately be needed.

What must be clearly recognized at this time is the need for smart cities to be protected from assaults on critical software and vital lines of communications that are absolutely vital to their functioning. Protection of key and highly automated infrastructure remains one of the top urban issues to be addressed and solutions found.

Unfortunately, an ultimate strategy to defend smart cities against cyber-terrorists with 100% success is not likely to be achieved soon. Efforts to create effective measures that are proactive rather than simply defensive in nature will take years to develop, but such measures are now critical.

Protective Actions to Fight Techno-Terrorists

There are many suggestions that could and should be taken with regard to protective strategies. Unfortunately many of these protective actions a lot of cost money and require technical expertise. Below are some of the many suggestions that urban governance leaders should seriously consider. Unfortunately a willingness to act to defend against techno-terrorists often comes only after a devastating attack—not beforehand, when it could have saved many lives and devastating losses.

- Use blockchain security in a systematic way, starting with its use in Internet of Things-enabled sensors and devices connected to urban infrastructure, as well as all vital command and control and key governance systems.
- Create independent hard-wired systems, not connected to the Internet, for the control of vital urban infrastructure, such as for water, sewage, transportation

© Springer International Publishing AG, part of Springer Nature 2019

J. N. Pelton, I. B. Singh, *Smart Cities of Today and Tomorrow*,
https://doi.org/10.1007/978-3-319-95822-4_12

systems, communications and IT networks, energy systems, nuclear power plant operations, etc., similar to those used in military and government installations and in some cities.

- Create independent electrical systems for military bases and other critical facilities using urban command and control systems. (Given the falling cost of solar, wind and other renewable energy systems, these steps could over time actually save operating expenses.)
- Review and upgrade the security for industrial control systems such as SCADA networks, under a single tech-savvy unit as well as conduct an independent audit of industrial control security practices.
- Engage in systematic security training for all city and relevant contractor personnel who are involved with the operation of vital urban infrastructure and its design and implementation.
- Improve processes and regulations to detect, report and respond to cyber-attacks against governmental authorities as well as to take defensive actions against such attacks.
- Recognize that natural disasters may create major problems in industrial control and automated governance and control systems, and engineer human-machine interfaces to allow intervention in advance of catastrophic events such as fires, tidal waves, and floods.
- Explore the vulnerabilities and do diagnostic forensics that are needed with artificially intelligent systems that might be attacked to prevent future attacks.
- Implement comprehensive data protection and governance structure and policies.

There is an elephant in the room that is seldom discussed when it comes to defending a country and cities against attacks by techno-terrorists. This is the fact that an invulnerable defense against secured and encrypted automated systems 100% of the time is truly never achievable because there are always new technologies evolving such as the Internet of Things and artificial intelligent control algorithms. Recently, vulnerabilities have even been exposed in computer chips that would allow potential hackers, especially so-called crackers, to invade chips and alter memories. These vulnerabilities are sometimes referred to as meltdown and specter. Meltdown and specter could theoretically allow a techno-terrorist to exploit CPU architectures and potentially gain access to protected memory in vital infrastructure. With billions of potentially vulnerable chips out there effective defenses become very, very, very difficult.[1]

Efforts to re-engineer computer chips and to use blockchain security to protect sensors and sensitive devices can help, but ultimately we must consider the reality

[1] "Meltdown and Spectre" http://www.aiaa.org/FebruaryProtocol/?utm_source=Informz&utm_medium=Email&utm_campaign=AIAA+Homepage Feb 14, 2018.

of human frailty that is built into all control networks. When humans are involved it seems no secret can be completely protected.

Cybersecurity thus comes down to the human weakness factor. Someone always has to know the security codes, and this vital information can be given away either through intentional treachery with criminal intent, or revenge-seeking malice or most likely, through trickery. Inside threats remain a major concern for government and corporate executives. Strategies to identify hostile hackers and techno-terrorists and then penetrate their identities also can never be achieved with absolute success in the age of the worldwide Internet. Further, a natural disaster can also bring additional devastation to an automated control system out of control. Thus, there must be a proper human-machine-interface to halt unsafe operations triggered or enabled by a fire, solar storm, tidal wave, or other catastrophe.

Absolute and complete protection of critical databases and highly secure IT networks and intranets against cyber-terrorist attack has, at least to date, been unsuccessful in each and every instance. Further, there must be new and increased attention to external attempts to thwart exploitation of hate groups by cyber-warfare attackers (including hostile nations), especially those who employ social media and fake news to stir up public opinion to undertake destructive acts. Such effort to use lone wolf extremists to undertake attacks on urban infrastructure or to rampage through pedestrian areas with a killer truck, such as was instigated by ISIS, remains a difficult task. This is particularly so when cyber-attackers or recruiters of terrorist attackers, can hide their identities through the clandestine use of social media.

Russian cyber-trolls apparently sought to manipulate the 2016 U. S. presidential election by stirring up opinion against Democratic candidate Hillary Clinton. Remarkably these types of techno-terrorists actually, in some instances, paid for their Internet hijinks with rubles. Some people even went so far as to suggest that payment to Facebook in Russian currency for such use of social media to stir up unrest was some sort of clue as to what was happening. We thought you had to be very clever to work at Facebook! In the age of bitcoin and other crypto-currencies members of extremist groups and cyber-attacks by hostile forces seeking to weaken democracy, or inflame racial or ethnic tensions, can, with equal ease, hide their identities and pay for their activities anonymously.[2]

Likewise, efforts to monitor social media sites that use encryption such as WhatsApp or Viper have not proved effective, even when new legislature has been passed to allow governments to intercept messages on these sites. In countries where various measures to allow their governments to intercept encrypted messages, such as in Germany, France and to a lesser extent in the United Kingdom, have unfortunately and ironically seen additional terrorist attacks ensue rather than lessen in number.

There always seems to be an additional way for terrorist cells to pass on secret messages. New ways to communicate secretly always emerge when troublemakers find their secret channels have been blocked. Ultimately the dark web seems to be

[2] Craig Tinberg, "Bitcoin boom is a boon for far-right extremists" *Washington Post,* Dec. 27, 2017, pp. A1 and A14.

available to cyber-criminals, techno-terrorists, or others seeking to achieve the covert exchange of information.[3]

Clearly new counterterrorist methods to enhance cybersecurity and digital defense are needed. In the remainder of this chapter we seek to explore what these new strategies might be. We particularly focus on methods that might be used to protect the key and often automated infrastructure that will be increasingly used in smart cities in the future. This protection now includes three approaches: (1) preventive access measures that use sophisticated blockchain encoding to protect key databases and networks; (2) diagnostics to identify intrusions in essentially real time; and (3) effective response measures to identify various types of intrusions and create response capabilities to restore systems from any aberrant behavior, various types of cyber assaults, cyber-thefts, or other digital attempts to intrude on key infrastructure.

Thus, there are both defensive strategies—that can only protect to a certain minimum threshold of security—and then proactive offensive strategies that can both respond to digital intrusions by restoring normal operation and services, as well as to target those bad actors that have been identified as harboring, encouraging or engaging in cyber-criminal or cyber-terrorist activities. Both these defensive and proactive offensive strategies will be examined below.

Defensive Strategies to Combat Terrorist Attacks on Smart Cities and Their Infrastructure

There are a number of defensive strategies that can be applied by cities to protect their vital infrastructure and their citizens from cyber-attack. Perhaps the most common and also a quite effective strategy is to have an encrypted code that is added for entering a protected database, control system, or highly sensitive IT network. There are guidelines that can be quite stringent in terms of using upper and lower case letters, numbers, symbols and to have entry codes being at least 20 digits long. For wireless smart phones new software that is dependent on facial recognition can also be highly secure. A combination of retinal scans, fingerprints, and entry codes can be highly protective of databases and software that control key urban infrastructure.

Another strategy that is used by security and defense agencies has been to limit access to sensitive information by not linking it to the Internet or other intranet so that intrusions into vita databases cannot be made by unauthorized personnel via the Internet. Such limitation to hard-wire access without being able to attain access via wireless systems clearly results in inconvenience, a lack of flexibility, and potential loss of quickly updatable "intelligence" into infrastructure of various types. The decision about who can access key databases and networks and the degree and

[3] James McAuley, "May Attacks Targets Cybersecurity in Britain" *Washington Post*, June 5, 2017 p. A9.

nature of physical access to these systems is a critical one. This is as important as the level of coded access and encryption associated with protected systems.

It is thus important to analyze the level of security of various key infrastructure. It is key to determine the degree to which automated control systems for smart infrastructure are physically isolated from wireless networking access or if specific protected access might be allowed for certain forms of mobile communications. Such an analysis would need to be undertaken on a case by case basis with regard to: (1) transportation systems of various types; (2) telecommunications and networking control and switching systems for governmental, education, and health services as well as for first responders; (3) distribution networks and storage facilities for energy and power systems of various types (i.e., electrical, natural gas, nuclear power, solar, wind or other renewable power systems); (4) water purification and distribution systems; (5) sewerage and storm water systems; and (6) any other database, billing system, or vital information or control system deemed vital to urban operations and services that might be subject to hacker or techno-terrorist attack. In many ways intelligence within a city's key infrastructure is now often at odds with cybersecurity.

Several examples involving current urban infrastructure vulnerabilities can be cited to illustrate the point. These examples are

- A U. S. east coast city has created under federal funding a smart transportation system by installing a broadband fiber optic network along all of its major thoroughfares with traffic signals. Today it is able to utilize a smart SCADA system to control strategically its traffic light signaling system to routinely speed rush hour traffic flow. In the case of a major D. C. terrorist attack this system could be used to facilitate emergency evacuations, whereby outgoing lights are changed to green. This system can also be used to allow express buses via a Wi-Fi system to activate the control of traffic signals. During an emergency or large traffic accident or fire, specially authorized first responders can activate the electronics in strategically placed traffic signals to create a Wi-Fi-based communications center. All of these capabilities are obviously of great benefit in all of these special use circumstances. A terrorist with the access codes to penetrate the smart traffic signaling system that could control this type of smart transportation and communications capability could create a great deal of harm. Traffic signals could all be turned to green in all directions and create a community wide rash of accidents and snarl traffic for an entire city. This could impose gridlock on an entire city.

- In Colorado some of the interstate highways are equipped with de-icing heater systems to melt ice and snow in the high passes and tunnels in the Rocky Mountain high elevation areas of the state. There is also an electronic sign messaging system to warn motorists of dangerous conditions such as a land or snow slide that has closed a road or other severe hazards. Again, if someone could seize control of these systems, while creating a hazard such as a snow slide or emptying a water truck's content in frigid conditions at the entrance to a high pass tunnel, there could not only be instantaneous chaos but commerce and food supplies could be shut down for some time.

- Train and subway systems in most major cities around the world have switching systems to allow single tracking of trains when repairs are being made on the tracks or there is an accident or failure of a train on one of the tracks. On most modern systems the switching and routing of trains is by computer, and human controls at the switch are undertaken only in emergency or special cases. If a terrorist could assume control of a train or city subway system especially during rush hour or in a case where a train carrying hazardous cargo could be made to derail, the consequences could be devastating not only in terms of lives lost but also longer term environmental damage.

These three examples concentrated only on cyber-attacks on various types of transportation systems. But they represent only one type of infrastructure vulnerability. Unfortunately it is likewise possible to use cyber-attacks to disable, disrupt, or even initiate lethal assaults on various types of urban infrastructure. Thus parallel types of cyber-assaults could, for instance, also be made on energy/power systems, water and sewage systems, and communications networks. In many cases such cyber assaults could lead to consequences that are even more dire.

Within a modern smart city the vulnerabilities are widespread and extensive. Airplanes, electrical power transformers, nuclear power plants, water purification equipment, sewage treatment plants, elevator and escalator systems, traffic lights, long-distance pipeline systems, and much more are today largely automated in their operation. As we move to driverless cars, trucks and buses, fully automated buildings with heating, ventilating, and air conditioning systems (HVAC), plus lighting, electrical systems, gas lines, and plumbing, even various forms of law enforcement and firefighting tasks operating under artificially intelligent systems, the cyber vulnerabilities will increase. As the Internet of Things becomes the Internet of Everything, the entry points for cyberterrorists and cybercriminals will increase exponentially. This strongly suggests that entry point security is the first line of defense, but that the ultimate line of defense must be to halt or limit automated systems when they embark on operations that put humans, or life-sustaining activities or facilities, at risk.

In short, innovations associated with smart city technology are all moving toward automation through the addition of expert systems and artificial intelligence to control and activate switching commands controlled by elaborate software. Such installation of smart automation serve to increase flexibility and creatively control the operation of urban infrastructure in order to make it lower in cost, more efficient, more reliable and generally safer. This is all true, unless there is a cyber-breakdown or a techno-terrorist attack on the software that controls this infrastructure. Various levels of cyber-defense must be created to prevent cyber-assaults at entry points, within operational systems, and especially with various types of monitoring systems to detect cyber-assaults and allow first-responders, IT systems engineers, or urban officials to assume control and be able to shut down automatons that are out of control or engaged in harmful operations due to cyber-attack.

It is, in most cases, still safer and more reliable to have communications or IT systems in control of most operations. A human operator that is capable of operating at 99% efficiency and with only 1% error is highly exceptional. A computer or digi-

tal communications system can consistently perform at 99.9999% accuracy or even much better reliability. A high-quality fiber optic cable, for instance, can be expected to transmit information with a bit error rate of 10^{-15}, say one error in a quadrillion. This is a reliability and resilience that no human has ever achieved. Machine intelligence and digital telecommunications is thus much more precise and reliable than humans. Yet, there can be a problem if someone tampers with the software or gets unauthorized access to a database and seeks to do harm. Then, simply because machine intelligence is so reliable and broadly relied on, things can go wrong if one installs malware, viruses, worms, Trojans, or other aberrant software that can disrupt, intercept, shutdown, or make destructive or even horrendous use of communications or digital processing networks. This might be done in order to steal money, acquire proprietary information illegally, or install dangerous instructions to computer controls in order to mount a terrorist attack. In light of the World Wide Web and the Internet such possible attacks just keeps growing in scope and geographic reach. As noted earlier in the chapter on the Internet of Things, the range of attack opportunities around the globe is growing exponentially.

There is a recently released report entitled "Connectivity is the Revolution," which is from the book *Geeks without Frontiers.* The purpose of this report and its supporting effort is to extend the reach of broadband systems across the entire global population of 7.5 billion people. This report and its associated "Community Connect" report estimates that there are as many as 4.2 billion people that lack access to the Internet via broadband systems. This report notes the many things that broadband services can bring, such as expanded education; health care' improved fire, policing and emergency care services; and better and more cost-efficient governmental services. It also notes the progress that is being made to upgrade broadband service in Africa, which is the most underserved region.[4]

It is ironic, however, that those without broadband and have limited telecommunications and Internet services are much better protected against all forms of cyberattack. It is useful for those planning broadband expansion to consider cybersecurity as an essential part of such expansion planning.

As can be seen in Fig. 12.1 there is a great disparity between usage in the most economically developed countries versus usage in the developing world, which is also characterized as the "Global South." As can be noted in Fig. 12.1, Internet usage is now quite extensive. Yet usage in Africa, in particular, lags behind the other continents. Africa, however, is currently the fastest growing user of the Internet with a 71% increase between 2016 and 2017.[5]

The other encouraging statistic is that the younger generation, in a systematic way all across the world, are using the Internet much more intensively. The follow-

[4] "Connectivity is the Revolution" Geeks Without Frontiers, October 2017 https://globenewswire.com/news-release/2017/10/19/1150375/0/en/Geeks-Without-Frontiers-Releases-Its-Community-Connect-Global-Broadband-Initiative-at-the-Geeks-Connectivity-is-the-Revolution-Thought-Leadership-Forum.html.

[5] ICT Facts and Figures, 2017, International Telecommunication Union (2017) http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf.

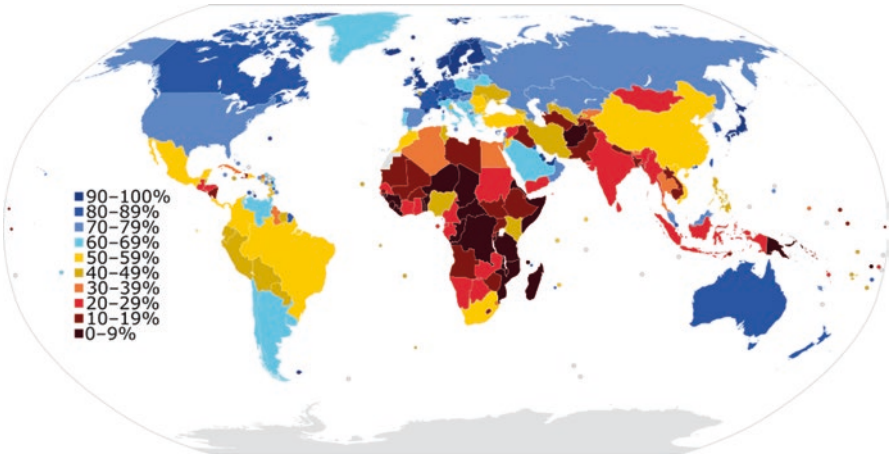

Fig. 12.1 Global profile of Internet usage as a percentage of total population (Map preparation by Jeff Ogden.)

ing report from the International Telecommunication Union provides a useful insight into global usage trends

> …young people are at the forefront of today's digital economy with 70 per cent of the world's youth being online. Today's ICT development is driven by the spread of mobile-broadband services. The growth of mobile broadband has largely outpaced that of fixed broadband, while mobile-broadband prices have dropped by 50 per cent on average over the last three years. These factors have resulted in about half of the world's population getting online and broadband services being available at much higher speeds. In 104 countries, more than 80% of the youth population are online. In developed countries, 94% of young people aged 15-24 use the Internet compared with 67% in developing countries and only 30% in Least Developed Countries (LDCs). Out of the 830 million young people who are online, 320 million (39%) are in China and India. Nearly 9 out of 10 young individuals not using the Internet live in Africa or Asia and the Pacific.[6]

This diversity in broadband access and Internet usage suggests that cyber defense strategies need to be adjusted and adapted to national circumstances. Yet global banking and commerce is vulnerable at all entry points. This means that the strengthening of cybersecurity in the less developed countries should be considered a priority, as access is extended globally.

In parallel a review of cybersecurity in developed countries has concluded that it is smaller businesses that have the greatest vulnerability to cyber-attacks. A survey of firms has shown the following types of concerns with regard to attacks in terms of priority from top to bottom (Table 12.1).

This list, which was prepared by the Financial Industry Regulatory Authority (FINRA), is perhaps a good summary of potential threats to smaller companies in developed economies. Yet such a list can also be used by developing nations in cre-

[6] Ibid.

Table 12.1 Cyber threats to industry

Priority rating	Description of concern
1	Cyber-risk of hackers penetrating systems for the purpose of account manipulation, theft, defacement or data destruction
2	Operational risk associated with environmental problems (e.g., power failures) or natural disasters (e.g., earthquakes, hurricanes)
3	Insider risk of employees or other authorized users abusing their access by harvesting sensitive information or otherwise manipulating the system or data undetected
4	Insider risk of employees or other authorized users placing time bombs or performing other destructive activities
5	Cyber-risk of non-nation states or terrorist groups penetrating systems, for example, for the purpose of wreaking havoc
6	Cyber-risk of nation-states penetrating systems, for example, for the purpose of espionage
7	Cyber-risk of competitors penetrating systems, for example, for the purpose of corporate espionage

ating digital defenses against hackers that might attack their financial institutions or governmental agencies. These seven types of cyber-risks are, in fact, rather universal around the world. It is perhaps significant that terrorist attacks are considered fifth out of the top seven ranked concerns in the FINRA survey of industry.

The fifth-down level of concern, in all likelihood, is a signal as to the expected infrequency of such attacks. Yet, the scope and scale of such cyber-assaults by terrorists when actually mounted can be devastating in their impact. There is clearly a problem in defensive strategy if less than one in a hundred of all attacks are mounted by techno-terrorists, but in this highly unlikely circumstance, the scope of the assaults is widespread, and the impact is devastatingly large.[7]

It is very, very difficult to create a foolproof defense against illegal or terrorist attacks on digital communications systems, on vital networks that store vital information or distribute strategic commands, or on those computer control systems that manage key infrastructure. In fact, in the age of the Internet of Things, this challenge is becoming more difficult every year. In short, computer network security is not easy. The rub is that most defensive steps to enhance cybersecurity limit the effectiveness of computer controls and automation. There is almost always a tradeoff. Upping computer and networking security will nine times out of ten limit the cost savings and efficiency offered by a higher degree of automation and industrial control capability.

Almost all defensive efforts to up one's game in terms of cybersecurity has the effect of limiting the intelligence, the functionality, and/or the flexibility of an infrastructure or system when you do any one of the following: (1) impose more controls on access, (2) limit the pool of people that can upgrade or improve the system, or (3)

[7] Small Firm Cybersecurity Checklist, Finanical Regulatory Agency, http://www.finra.org/industry/small-firm-cybersecurity-checklist.

restrict access to the system via only direct or hard wire, non-switched access to a data system. This means that fully protected databases are completely isolated and physically separated from other networks or allow only highly encoded and extremely limited access via any wireless communications access system.

In conclusion, we can say that defensive systems to prevent abuses or assaults on smart infrastructure are quite possible. All industrial control, smart SCADA, and control software for all smart software should be protected through stringently encoded passwords. In one community, where a security audit was undertaken of industrial control systems, it was found that security for such systems was distributed among at least four operating units of government and that access codes were not stringent, regularly updated, and in some cases had remained the same from the start without changing the manufacturer's default code. The result was to consolidate security for all urban infrastructure in a unit that was tech savvy and charged with instituting new stringent, long and complex security codes that were updated at least twice a year if not more frequently and an outside security consultant was charged with an annual review of all the city's cybersecurity operations. A parallel review was undertaken of the switching centers for the telecommunications carriers that serviced the local government and school system, the 911 call center and services to the local police, fire, and EMT dispatch facilities.

Proactive Offensive Strategies to Combat Terrorist Attacks on Smart Cities and Their Infrastructure

North Korea has been identified as the likely backer of the WannaCry ransomware deployed in 150 countries involving over an attack on over 300,000 computers, including an assault on the UK's National Health Services (NHS). This type of crippling attack is even more alarming if it is seen not as a single stand-alone incident, but rather if it were considered to be a sort of a training exercise for a truly global cyber-warfare attack. If mounted in a full-scale way such an attack could potentially cripple the global economy and shut down vital services such as health care, electrical power and communications networks.[8]

It is thus critical to develop proactive and offensive capabilities to cope with future cyber-attacks. This means being able to detect intrusions and attacks, and to be able to counterattack by shutting off the offending digital network and perhaps disabling the originating site. It clearly involves restoring the attacked computer systems to their pre-attack status and to creating new protective systems, codes, encryption capabilities, and firewalls to prevent a recurrence of similar attacks.

This returns one's attention to the U. S. National Institute of Standards and Technology (NIST) Cyber Security Framework that is again provided in Fig. 12.2 below.

[8] Researchers See Possible North Korea Link to Global Cyber Attack, AOL News, May 15th 2017, https://www.aol.com/article/news/2017/05/15/researchers-see-possible-north-korea-link-to-global-cyber-attack/22088395/.

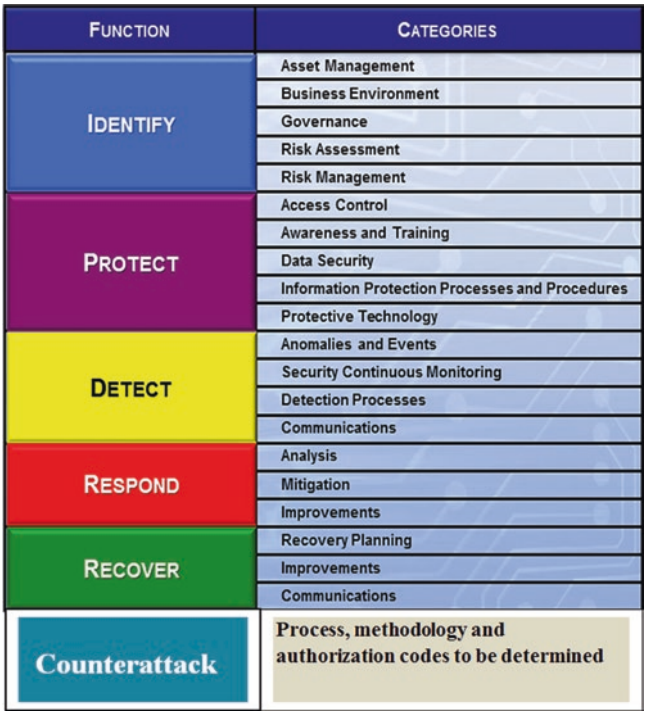

Fig. 12.2 Proposed augmentation to U. S. NIST cybersecurity protocol

This is provided again for ease of reference and to note its criticality. In this new proactive mode one would add a sixth step. Thus, the revised protocol would include: (1) identify, (2) protect, (3) detect, (4) respond, (5) recover, and (6) counterattack. The counterattack process would be under the control of governmental defensive agencies, and it would first seek to disable the site as was ultimately achieved in the case of the WannaCry attack, but also find the most effective means of counterattacking so as to bring the cyber-attackers to justice.

The concept of counter-assault to close down attacking sites and arrest and to bring to justice those carrying out international assaults on vital computer networks is not something that a single nation would or should carryout unilaterally. The methodology and international process whereby this would be done would need to be coordinated to ensure that this would be carried out after a determination of a terrorist assault deemed to be considered equivalent to an act of war. The international process to coordinate national defense cyber counterattacks would require careful discussion and agreement. Key to this process would be the Internet Society, the Internet Engineering Task Forces, the European Agency for Network and Information Security, the Japanese Cyber Security Initiative, the U. S. NIST, and other coordinative bodies that address cyber security issues. It would also likely require amendment to the OECD guidelines for the Security of Information Systems, plus laws in the United States, Japan, China, Russia, India, Canada, Mexico, Brazil, Argentina, Egypt, Nigeria, South Africa, Australia, and New Zealand, just for starters.

This is a process that will clearly take some time and could entail changing some of the basic architecture of the Internet and intranets around the world.[9]

The U. N. Charter in Article 2(4) explicitly forbids states from engaging in the "threat or use of force against each other" or in effect rules out warfare. But what Article 2 forbids, Article 51 partially restores. This Article 51 states that this charter does not forbid the "inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."[10]

Further the U. N. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, known as the Outer Space Treaty, provides that states shall not place nuclear weapons or other weapons of mass destruction in orbit or on celestial bodies or station them in outer space in any other manner.[11] Despite these admonitions for peaceful activities and respect for human rights contained in the U. N. Charter and the Outer Space Treaty, as well as the asserted rights of individuals proclaimed in the U. N. Universal Declaration of Human Rights, wars, attacks on other nations and various assaults on people and institutions continue to take place. In the Internet Age, attacks on countries can be carried out not only by armies and physical assault but also via IT networks via malware. When Leon Panetta was Secretary of Defense during the Obama administration he warned of the coming likelihood of a cyber-attack on the United States that was the equivalent of an electronic "Pearl Harbor" that could have devastating effect.

During the latter half of 2017, at the height of the seeming hostilities there was a great deal of news about the possibility of a nuclear confrontation between the United States and the Democratic People's Republic of Korea that could involve nuclear missile exchanges or actual physical assaults. The revelations that North Korea was actively involved in the so-called WannaCry ransomware attacks in May 2017 also raised the issue of a possible cyber-war involving the United States, North Korea and potentially other nations. There were concerns North Korea was preparing to launch a major cyber-assault on key infrastructure and institutions in America and other nations. Thus there is an unresolved question as to what recourse there might be to such a situation if it actually occurred. Today the threat of a U. S. and North Korean conflict has seemingly abated, but the question remains as to whether cyber-warfare is an act of war that can or should be equated to an armed assault or the launch of missiles against a state.

In today's world there is no clear answer to the status under international law of pre-emptive strikes in self defense. There is now also a subsidiary question that is posed by the intensive use of modern electronic technology and IT control systems

[9] Joseph N. Pelton and Indu Singh, Digital Defense (2017) Springer Press, New York (see appendices).

[10] Charter of the United Nations http://www.un.org/en/charter-united-nations/index.html (last accessed Oct 24, 2017).

[11] Outer Space Treaty http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html (last accessed on Oct 24, 2017).

as to what is the status of international law with regard to pre-emptive cyber strikes. In short the subsidiary question is, what if there were to be a creditable threat of a major "Pearl Harbor type electronic cyber-attack" on the United States by North Korea or some other techno-terrorist group? Should the U.S. engage in a "pre-emptive cyber attack to "defend" itself? And if so, on what precedent under international law might this be done?

Here the status of international law is murky at best. The discussion by international legal jurist usually centers on what might be done about potential nuclear strikes or other attacks on physical infrastructure. There is no real international law or useful precedents about potential strikes against hackers or techno-terrorists that might use data networks to carry out attacks against individuals, commercial organizations or institutions, or even national governments.[12] Today hackers or abusers of the dark web are tracked down, arrested, and go to trial to determine their guilt or innocence. Protective strategies are taken to defend databases and key electronic networks and infrastructure, but there are limited abilities to engage in retaliatory strikes, and no legal, regulatory, or other basis to carry out a pre-emptive cyber-attack to defend oneself.

If another attack similar to the massive WannaCry attack were to occur in the future, it seems likely that systematic counterattacks would very likely occur. Indeed there might well be consideration given to authorizing pre-emptive strikes against threatening global capabilities. Today a physical attack by an invading army, a missile, a rocket or a tank assault is grounds for declaring war on the attacker and launching an active defense under Article 51 of the U.N. Charter. There is a need to clarify whether a nationally-backed cyber-attack on another country is indeed an act of war and that Article 51 of the U.N. Charter comes into play. Further it seems clear that cyber-defense will involve removing and possibly destroying the capability of the attacking party to continue to disable smart infrastructure, or continue an ongoing cyber assault. This is today a gray area as to at what level does a cyber-attack by a rogue nation or entity such as ISIS constitute an act of war. An even grayer area is can a nation protect itself by making pre-emptive strikes against cyber-attackers whether they be another country, a techno-terrorist entity or a criminal organization. A similar question is whether an attack on vital satellite infrastructure such as a communications satellite, a remote sensing satellite or a space navigation satellite similarly could or should also be considered an act of war.

In order to establish an effective global system to locate and counterattack techno-terrorists around the globe will require some degree of international cooperation. National governments and their police and defense forces will need to play a key part in enforcing cyber-countermeasures within their own countries. Currently the only international agreement on this subject is the European Union's Convention on Cybercrime signed in Budapest, Hungary, in 2001 and which entered into force in 2004. As of the end of October 2017 it had 56 signatories including most of

[12] Alex Potcovaru, The International Law of Anticipatory Self-Defense and U.S. Options in North Korea. Lawfare, August 8, 2017. https://www.lawfareblog.com/international-law-anticipatory-self-defense-and-us-options-north-korea (last accessed Oct. 28, 2017).

Europe and the United States. This international agreement is the most comprehensive convention currently in effect with regard to cybersecurity. It includes crimes committed via the Internet and other computer networks and covers many different areas of criminal behavior in cyberspace including such matters as violation of trademarks and copyright, computer-related fraud, child pornography and many other matters that involve violations of network security and all forms of cyber-theft. Perhaps the most significant aspect of the Budapest Convention is that it also contains a series of powers and procedures whereby governmental enforcement authorities are potentially enabled to carry out searches of computer networks and to intercept cyber-criminal or cyber-terrorist messaging.[13]

Most recently Russia has developed a draft of what is entitled a United Nations Convention on Cooperation in Combating Information Crimes, and this proposal has generally raised concerns among a number of Western governments and especially the United States. The Russian proposal has been characterized by U. S. cyber-experts as a means for "…Russia and other authoritarian governments to control communications within their countries, and to gain access to communications in other countries."[14] A U. N. group of experts on information security ceased to meet in June 2017 after failing to reach any meaningful agreements. In the case of Russia, their primary objection to the Budapest Convention is that in Article 32 (b) of the text it declares that the private owners of information are designated protection and proprietary control as opposed to governments having primary control and ownership of information.

The latest development in this arena is a September 2017 resolution by the Brazil, Russia, India, China and South Africa (BRICS) that indicated agreement on the "need for a universal regulatory binding instrument on combatting the criminal use of ICTs (Information and Communications Technologies) under the auspices of the United Nations." The problem is that in U. N. processes unanimous agreement on conventions is needed. In the Internet arena there is wide disagreement as whether governments or individuals should control information ownership and use. This gap in opinion suggests that no universal convention on cybersecurity will be negotiated and agreed upon soon.

The fundamental issues associated with cyber warfare is that it can act as a great equalizer among nations with great resources and military might and those with a limited military and modest financial resources. North Korea, Iran, and other nations have mounted attacks against the United States, and proof of such attacks is hard to develop. Even finding the likely culprit can take days, weeks or even months. The worldwide WannaCry attack had the clear fingerprints of North Korea on it. A recent Carnegie study of Iranian cyber-warfare tactics entitled "Iran's Cyber Threats" detailed Iranian attacks on U. S. banks and Saudi Arabia's Aramco. This attack used a virus known as Shamoon. Ironically this virus was similar to that purportedly used

[13] E.U. Convention on Cybercrime, European Treaty Series 185, Signed in Budapest, Hungary Nov. 23, 2001 entry into force on July 1, 2004 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[14] David Ignatius, "Russia Plots a New Cyberwar Front", Washington Post, Oct. 26, 2017, p. A. 21.

by agents of the United States to attack the Iranian nuclear program. Thus cyber-warfare attacks and counterattack responses can escalate over time, a situation recently summed up as follows: "Iran has an arsenal of cyber-stones, so to speak, ready to throw. The United States, meanwhile, lives in the world's biggest glass house."[15]

And beyond these legalistic or regulatory questions, there are, of course, quite valid technical questions as to whether those undertaking—or planning—cyber assaults can be correctly identified and located with precision so that such a response—or pre-emptive counterstrike—is indeed possible. Some who are involved in cybersecurity enforcement might seek to divide offenders into prankster hackers, cyber-criminals, and techno-terrorists, but in terms of detection of intrusions, cybersecurity protective measures, and even counterattack methods, the technology does not differ.

Is a "Bot" Attack Via Trolls a Techno-Terrorist Attack?

Yet another issue that is perhaps even more imponderable is the use of bots and social media not to launch attacks on urban infrastructure but rather to influence and distort public opinion and voting patterns within the electorate. The manipulation of public opinion through the use of bots and ads on social media has come to light in terms of investigations of the Russian interference in the U. S. presidential elections of 2016. But this is not in any way an isolated event. Studies conducted at Oxford University in the United Kingdom after the U. S. presidential elections of 2016 found that between the first and second presidential debates there were numerous online posted comments that came not from people but bots that were seeking to influence the election. Reported estimates from the Oxford University study was that "more than a third of pro-Trump tweets and almost a fifth of pro-Clinton tweets came from bot accounts." Some analysts fear that this weaponization of the Internet via bot account posting is ultimately a threat to democratic elections and a distortion of public opinion within a community, a region or even an entire country.[16]

This is a topic largely beyond the scope of this book but is one that must ultimately be of concern to political leaders of those seeking to create smart cities that are responsive to its citizenry. Political leadership that cannot get accurate and reliable information as to what its citizens think, feel and want cannot design and implement what is truly a smart city. If trolls and bots distort what the public wants and feels in communications with political leaders, it becomes an impediment to the effective operation of a smart city.

---

[15] David Ignatius, "We shouldn't ignore Iran's cyberthreat" Washington Post, December 27, 2017, p. A13.

[16] John Herrman, "On Technology: Technologists once told us that social bots would change our lives forever. They were right, but not in the way they expected" *New York Times Magazine*, November 5, 2017 pp. 14–17.

Artificial Intelligence and Techno-Terrorist Attacks

Another final issue and concern revolves around the increasing use of artificial intelligence in self-driving cars, in smart transportation systems, and in smart urban infrastructure. There was a probing article entitled "You Can't Ask a Self-Driving Car Why It Crashed" that began with the puzzle about what an artificially intelligent program "thinks" when it makes the wrong decision that leads to a self-driving car to crash, as was recently the case in January 2018 in Pittsburgh, Pennsylvania, and in March 2018 in Tempe, Arizona. This article noted that humans for "ethical, social, or legal" reasons are asked to explain the basis for their decisions in life when it comes to the exercise of judgments, but that AI algorithms are not currently engineered to be able to explain whether they mistook a yield sign for something else or could not distinguish a whitish truck from the open sky.[17]

The question that arises is whether AI programs could be designed to store information about their decision-making processes. Presumably this would allow an AI algorithm to be queried and even to defend itself in something like a court of law. This type of next step in AI design would allow for smart algorithms to keep track of all actions, including key decisions that they had made, particularly those with a life and death consequence. This is clearly a very tricky area where AI programs—or presumably their program designers—might be put on trial at some future date. If we were to travel forward into a world where robots were controlled by something like Isaac Asimov's three laws, where they are compelled to save humans and not take an action that might harm a human, then something like this process would seem necessary. This type of ethical issue for AI designers become more and more germane as we see the evolution of AI from the control of the steering, braking, and acceleration of cars, to the routing of traffic and control of traffic signals, or to the running of nuclear power plants.

And what about one day in the future when there are operational bot soldiers, like in the world of *Star Wars* that engage in fighting on the battlefield. Again this is an issue beyond the scope of this book. The ultimate question here is whether the designers of AI algorithms have a responsibility of creating 'memories' of all decisions that a bot might make so that key actions, including those with life and death consequences, can be explained and ethically and logically defended in a future inquiry, much like a court of law. And if this were to be the case, what about a future with warrior bots that are charged in a sort of Nuremberg trial? Who would be in the dock—the bot or the designer of the AI program?

The bottom line here is that AI systems are growing more and more powerful and pervasive each day. They will play a key role in the design of future of smart cities and in the possibility of remotely located techno-terrorists being able to attack and potentially inflict great harm to the operation of world urban centers. When do such attacks become an act of war? And if the attacked or the attacker involves the use of

[17] Finale Doshi-Velez and Mason Kortz, "You Can't Ask a Self-Driving Car Why It Crashed" *Washington Post,* March 25, 2018, Outlook, P.B1 and B6.

AI technology, who is ethically and legally at fault? In this strange world a future AI program might be developed by an American, enhanced by someone from China, and then used by someone in yet another country such as North Korea to attack a European city with devastating effect. Who is responsible?

Conclusions

What is changing is the level of sophistication of attacks and the complexity of defense in the age of the Internet of Things, which is morphing into the Internet of Everything. With the exponential increase in Internet traffic, the volume of use that involves machine to machine traffic, and the huge increase in wireless-based traffic that comes with 5G (fifth generation mobile) urban security, the protection of protected smart infrastructure will become increasingly difficult to achieve, especially via defensive strategies alone.

In looking to the future of cybersecurity for smart cities there are two things that seem to be essentially true.

1. Cyber vulnerabilities will increase and not decrease. Both criminal and terrorist activity online will be harder to detect and prevent and will spread around the world, especially to countries that are lenient in their prosecution or are perhaps rogue states. The role of countries such as the Democratic People's Republic of North Korea or those that harbor ISIS terrorists must be of particular concern.

2. Prevention or limitation of cyber-attacks via defensive measures (such as more stringent passwords policies and use of blockchain encoding, facial and/or retinal recognition systems, firewalls, anti-virus, and encryption) will be ever more difficult to achieve. Thus active measures such as sting operations, defensive viruses, and improved tracking systems to locate cyber-attacks and especially defenses against distributed denial of service (DDOS), etc., will be needed. Also smart infrastructure that is critical to the operation of vital urban and national systems may need to be physically isolated from Internet access for vital protection. Likewise, more and more decentralized energy systems with renewable energy sources may make sense for several reasons. These include: (a) protection of energy infrastructure and resilience, (b) reduction of operational costs, and (c) reduction of a city's carbon footprint and pollution levels.

All of the strategies outlined in this chapter should be actively explored and possibly implemented at the national, state or city level.

Chapter 13
Flexibility, Vision and Foresight in the Planning for Tomorrow's Smart City

As a sage wag once observed: "The future is not what it used to be." We truly live in a time of future compression, where change sometimes seems to be spiraling out of control as we zoom into Tomorrowland. Planning for a smart city that has sufficient legs to remain current for even a few years seems incredibly difficult. How can city planners have the insight of an Arthur C. Clarke or a clairvoyant to design smart cities that remain vital for even as long as several decades into the future? Technological innovation, social interaction on the Internet, globally linked economies, and increasing trade in services and intellectual property in today's digital ecosphere are all combining to accelerate the rate of change. The concept of an increasing rate of acceleration is known to physicists by the highly technical term known as jerk. That is the term for a fourth order exponential of change over time.

Jerk is represented in the physical world as what happens when you stomp on the accelerator and put the pedal to the metal of a hot rod or a bomb explodes. The bottom line is that it is increasingly hard to keep up in today's world of technical jerk. For urban planners, where millions of dollars are being invested in infrastructure that might become obsolete in 5–10 years, the challenge of making the right decision is truly enormous. Flexibility, vision and foresight are three crucial tools to use in planning for a smart city that can have some staying power.

How do you design a smart city so that it remains responsive to the complex and changing demographics of a dynamic urban landscape that is constantly in change? How do you create a smart city that remains capable of meeting fluctuating social and economic conditions for many decades into the future? With the rising concerns related to climate change and global warming there is the need to adjust to other conditions such as weather and longer term environmental changes.

Also there is the requirement to consider the city's need to adjust to a changing populace that responds to the needs of senior citizens, millennial and Gen-Xers. The infrastructure requirements can be quite different for different sectors of the population when it comes to transportation, communications, housing, education, health care, recreation, physical fitness and various types of demands on first responders. It is thus necessary in creating a truly smart city to create infrastructure that is

© Springer International Publishing AG, part of Springer Nature 2019

J. N. Pelton, I. B. Singh, *Smart Cities of Today and Tomorrow*,
https://doi.org/10.1007/978-3-319-95822-4_13

efficient and cost-effective but also flexible enough to respond to different parts of the populace as well as to changes over time. Can the smart city respond effectively and efficiently if there are key shifts in socioeconomic or even environmental conditions? In designing this flexibility and adaptability into smart infrastructure and automated services driven by AI algorithms, there is also the vital aspect of cybersecurity and natural disasters that likewise must be considered. In short, greater flexibility and responsiveness could also lead to better urban design that allows smart cities to have a much longer shelf-life.

To design a city with flexibility, vision and foresight involves more than seeking to anticipate future trends in technology and human innovation. It also requires understanding possible longer-term vulnerabilities and issues such as demographic variations. Below is but one such example of the type of long-cycle variations that smart city planners should take into account.

In 1859 the massive solar storm known as the Carrington event occurred. This was a massive coronal mass ejection of solar ions that raced from the Sun's corona at millions of kilometers an hour. When these ions blasted Earth they knocked out telegraph offices and even set fire to paper in these offices. At the time telegraph services were the only electronic infrastructure in operation in the entire world. Today electronic systems are essential to most forms of urban infrastructure. Electronic controls, gates, switches, machinery, satellites, spacecraft and networks are vital elements of everything that allows modern cities to operate as they do. At risk when extreme solar storms occur are transportation systems, energy plants and distribution grids, communications networks as well as such vital infrastructure as traffic signals, pipelines and even water and sewage systems.

Satellite systems in the skies are now vital to navigation and control systems for aircraft, ships and all sorts of vehicles. They also provide communications, networking, weather monitoring, precise timing services, and hundreds of other functions from resource prospecting to a wide range of policing and defense operations.

Electronically linked and controlled infrastructure—so pervasive in modern society—are vital to the modern city and the normal operation and day-to-day employment of the great bulk of urban employees. Urban designers must be aware that natural catastrophes and events such as solar storms, shifts in Earth's magnetosphere, asteroid strikes, volcanoes, earthquakes, and floods can likewise wipe out vital infrastructure as well. A Lloyd's of London study of the consequences of a major coronal mass ejection (CME) estimated the potential damage might be on the order of $3 trillion. Indeed the subsequent loss of life could be staggering, but fatalities from failed transportation and communications systems were not estimated in this study. And this is just one aspect of how urban planners must look to tomorrow and the design of smart cities in new and fresh ways.[1]

Of course, a Carrington event-type of catastrophe represents just one of seven "black swan" type of mega-catastrophes identified by the National Intelligence Council of the United States, as the type that could impact our planet and especially

[1] "Lloyds of London warns-of devastating 2.6-trillion solar storm" Wind.com. December 4, 2016. http://www.wnd.com/2016/12/lloyds-of-london-warns-of-devastating-2-6-trillion-solar-storm/.

challenge the viability of mega-cities with massive populations that depend on supply chains for food and electricity for their jobs.

On the other hand there is also the need to anticipate future opportunities or technological innovations. These might well unlock new options or create new possibilities to which a smart city might wish to exploit or respond to in a positive manner. New opportunities, however, can also give rise to new dilemmas and social, economic, and political problems as well. All of these what-if questions about threats, opportunities, and technical and social innovation are the types of challenges that planners of smart cities should take on seriously. The keys are flexibility, vision and foresight.

Learning to Anticipate and Cope with Change

Indeed there is a wide range of potential developments from social or technical innovations that could also reshape the future of modern cities. Here are just a few of the predictions for the near- to medium-term future that could reshape the direction of 21st century smart cities:

- Driverless cars, trucks and buses, driverless "hover" vehicles and drones, ride-sharing, telecommuting, and other improvements in transportation systems could result in less urban congestion, and the need for fewer roadways and car ownership in developed countries might be cut in half. Urban atmospheric pollution might as a consequence be reduced.
- The advent of large-scale drone delivery systems, "flying cars," high-altitude platform systems for communications, broadcasting and Earth observation, and possibly hypersonic space planes, may lead to a crisis in air and space traffic control and management and traffic safety in both urban and rural areas. (See Fig. 13.1.)
- Innovations in artificial organs, new medications, innovations in AI and widespread use of smart robots in medical treatment and disease diagnosis, could greatly extend lifetimes, with typical lifetimes being extended to 120–130 years of age. This could create a crisis in areas such as retirement benefits, social security and healthcare services, retirement ages for employment, and in other areas such as housing, transportation design, and a full employment economy.
- Concerns over the safety, the difficulty of first-responders providing emergency services for mega-high-rise buildings, improvements in broadband communications, innovations in virtual reality and telepresence, plus concerns about urban pollution, climate change, supply chains in emergencies, and inflated real-estate costs for super-dense cities, may all combine to alter the concept of central core density in urban planning. This might lead to the realization of the long-term

Fig. 13.1 Image of the Terrafugia flying car with a flight speed of 107 mph/172 kmph (Illustration courtesy of Terrafugia images.)

predictions of Arthur C. Clarke for tele-cities and help ease the pressure on mega-cities to reformulate urban architecture.

- Continued innovation in sustainable energy sources, particularly for solar cell and quantum dot technology, wind energy, and new energy storage systems, plus new passive energy systems, might also lead to rethinking of the structure of energy grids, district energy systems and innovations that could come with smart sensors and meter systems to lower energy costs and make them less vulnerable to catastrophic blackouts, with greatly reduced carbon footprints and lower energy costs.

These are just some of the future trends that might be anticipated in the coming decades, and these could greatly impact the architecture, design, costs, safety, and employment patterns that might be seen in a smart city in 2040 or 2050 and in some cases much earlier.

A failure in the cooling systems that destroys a nuclear power plant and causes it to melt down, the chemical or radiological contamination of an entire urban water supply or the deliberate sabotage of a city's sewage treatment plant could lead to the deaths of untold numbers.[2] And these are just some of the natural or manmade disasters that smart cities might need to cope with and respond to quickly and hopeful efficiently.

No, the strategy of the future must be a combination of planning for flexible infrastructure and systems, coupled with rapid and intelligent recuperative response. Most of all, a key element of smart city planning must be flexibility. Some urban planners are today so overly focused on cybersecurity that they overlook the need for safety and emergency response to natural disasters (i.e., earthquakes, solar

[2] Joseph N. Pelton "Our Changing Would and the Mounting Risk of a Calamitous Solar Storm" *Room Space Journal,* Summer 2016. http://room.eu.com.

storms, floods, hurricanes, typhoons, volcanoes, and droughts), manmade disasters and accidents (i.e., chemical or radiological spills, fires, train derailments, and industrial operator errors) plus equipment failures and infrastructure failures of pipelines, electrical grids, or failure of bridges, overpasses, dams, and other urban facilities that may well be a consequence of improper maintenance and failure to replace faulty infrastructure. One of the important ways to look to the future is proper maintenance and systematic upgrade, repair, or replacement of vital infrastructure. Sometimes a fascination with gee whiz new technology and the implementation of new gizmos leads to improper maintenance of infrastructure that has passed its nominal lifetime.

The past, the present and the future are connected. The needs of a smart city in terms of technological innovation are not clearly understood by city political leaders, planning staff or technical innovators. Some of the most important innovations are far from clearly defined in terms of performance versus extended lifetime versus cost efficiency.

It may be best for a city planner to urge for the design of a new and improved type of material for water mains, storm-water drains, or sewage conduits, equipped with performance monitoring sensors, with a 100-year lifetime rather than 30 years. This type of R&D challenge may be far more important to a smart city rather than perhaps to support the development of a flying car or hovercraft.

An installation of LED street lamps and pedestrian walkway lights might serve to reduce electricity consumption, but the true savings may be hidden elsewhere. In one city studied, the LEDs lasted 10 to even 15 years with an extended lifetime guarantee. Alternatively conventional arc lights lasted only about 18 months. The true savings came from the fact that it cost about $70 for a crew to replace the burnt out bulbs. Part of the smartness of a city is to be able to account accurately for capital, operating, repair, and maintenance expenses and understand the total cost outlays over time.

Development of a solar cell power system with a type of radiation shielding that can allow the unit to perform with reasonable efficiency for 50 years or longer, might be more important to a smart city than the development of a quantum dot solar generating system that is 20% more efficient than today's best silicon-based photovoltaic unit. This is to say that time cycles, maintenance and replacement of failing infrastructure is key. In some cases this means updating or replacing infrastructure. In other cases it may well be that the best strategy is to make infrastructure smarter—by imbedding systems with sensors and Internet of Things-enhanced devices. There needs to be a calculus to understand whether innovations are aimed at increasing performance, enhancing safety, or extending lifetime. The 'smartness' here is being able to establish and monitor performance via clearly understood guidelines.

Resilience Monitoring and Control

Effective planning and well-designed resilient systems with effective human-machine interfaces and efforts to avoid over-centralization and a lack of flexibility in urban controls can be difficult to achieve. Such flexibility of planning can help adjust to shifts in the population such as more school age students, an increase in the elderly, or an economic downturn. This same flexibility can also help mitigate the size and damage that might come from a terrorist assault or a major natural disaster. It is essential to plan for potential cyber-attacks and natural disasters with smart and flexible systems that can respond, mitigate and minimize the impact. This means that the top objective is to limit the degree of damage that can be done via well-conceived failsafe measures, which are even more important than preventive measures to ward off such attacks. First, second and even tertiary emergency response systems are needed to shut down the attacked systems to allow structured recovery processes to take hold and limit damage. This tiered "prevent system" is key to rendering smart infrastructure more resilient and better able to weather the most determined of cyber-attacks. If there is only one line of defense and only one way to respond to attacks or natural disasters, the probability of catastrophic attack goes up exponentially.

Optimization of Automated Urban Infrastructure

It should be abundantly clear that urban control and management systems should be designed with utmost care. The design of such systems should seek to include truly effective firewalls, access codes, facial recognition systems and encrypted and back up data systems so that they operate with a high degree of reliability, safety, continuity, and autonomy. The idea of using dedicated local area networks, insulated from direct connection to the Internet, which has been suggested by a number of experts, is a very good idea. Such insulation of vital infrastructure from the Internet makes any attempted attacks on vital urban infrastructure more difficult to attempt and incursions easier to detect. Such separation of vital systems from the Internet and isolation on dedicated intranets makes attacks easier to be initially rebuffed and thus do no harm in the first place.

Even so it is not a valid conclusion to assume that all vital infrastructure will be completely and effectively walled off from all attacks in every instance. In today's digital ecosystem this is wishful thinking. The objective is to reduce incursions to a minimum and to be able to track down any and all attackers within a limited range of opportunity.

In addition, there must be additional efforts to limit and isolate the damage through modularity of design and operational defense lines to segregate large systems into modular units as the second line of defense and to isolate viruses or malware as a counter-response takes hold. This ultimately means that urban planners need to coordinate with cyber-defense and law enforcement to undertake proactive

measures to detect and prosecute cyber-criminals and techno-terrorists to halt assaults on computer networks and automated control systems. There are many models to follow in this regard. The defense systems against financial intrusions and market manipulation as practiced within the Security and Exchange Commission is but one case in point.

The usual approach that a system's engineer takes in designing a complex system is to seek maximum efficiency. This usually involves creating the simplest possible system with the fewest components where most if not all redundancies are eliminated. Further, the minimum tolerances must be consistent with performing the desired mission. In designing the operation and controls for vital infrastructure of the smart city, the approach should not be that of the system's engineer seeking maximum efficiency. Rather the mindset should be that of a safety engineer who seeks maximum reliability, elimination of single points of failure and checks against system failure and terrorist attacks. Modularity of design with the ability to shut off and isolate attacks, accidents, disruptions or natural or manmade faults or accidents should be the guiding principle.

In designing smart systems, whether for today or tomorrow, it is critical to become rapidly aware that some sort of attack, natural disaster, accident, or service disruption is occurring and then being able to revert to a "safe mode" as quickly as possible. This should include being able to sound alarms to first responders—i.e., both through human and computer controlled systems—as soon as possible. Such a system should convey clear information as to what form the attack is taking and what appropriate responses should be taken, subsystem shut down or linkages shut off. This will require the ability to constantly update protective software in order to be able to detect various types of attacks and create appropriate levels of safety response modes against such attacks, accidents or natural disasters. In designing systems to be modular, resilient, and able to detect incursion or malfunction it is important to note that causes such as fire, flood, earthquake, equipment failure or operator error may well be more likely than a terrorist attack.

Designing Flexibility into Urban Infrastructure

Some architects of smart cities see their role as simply to automate the urban infrastructure in order to cut costs and improve reliability of operations. There is nothing wrong with these objectives, but these goals by themselves are much too limited. The start of the process is actually to understand more clearly the current and future needs of the community that is to be served. This may translate into preserving options, or modularity of design, not tying urban services or future design considerations to a single aspect of the overall urban demand. Today most cities are designed around transportation networks. In the future broadband information and mobile communications networks may create new and more flexible options. Conduits and corridors for IT and entertainment networks, water, sewage, electricity, natural gas,

Table 13.1 Listing of major big data analysis firms (courtesy of Datamation)

The Datamation listing of 25 top "Big Data" firms
Tableau, New Relic, Alation, Teradata, VMware, Splunk, IBM, Striim, SAP, Alpine Data Labs, Oracle, Alteryx, Splice Machine, Pentaho, SiSense, Thoughtworks, Tibco Jaspersoft, Amazon Web Services, Microsoft, Google, Mu Sigma, HP Enterprise, Big Panda, Cogito, and Datameer.

and transportation should be looked at in the context of integrated networks rather than as a dozen unrelated grids and channels.

The first step is thus to collect a good deal of relevant data and analyze it against a predictive analytic model to see what the interaction of these key drivers will produce over time. Some of the parameters that should be clearly monitored and understood are:

1. Demographic data and especially demographic trends in terms of aging, people coming and leaving the community (both in numbers and characteristics), etc.
2. Budgets and budget trends (local, regional and national)
3. Economic data for industries of interest and of various relevant classes of residents.
4. Employment trends and changes in types of jobs available and any declining sectors.
5. Infrastructure data (condition and degree of automation and industrial control, age and when latest updated or modernized or retrofitted).
6. Trends in energy systems (stand-alone solar power systems for homes and businesses, district energy systems, smart meter systems that allow selling of energy back to the grid, modernization of the grid to make it smarter, etc.) and then seek a design that allow for more modular flexibility.
7. Climate, geological, environmental, and weather conditions. (This should particularly highlight coastal conditions and any factors related to annual flooding, earthquake concerns and atmospheric and water pollution concerns, etc.)
8. Other surveys of particular interest including patterns of cyber intrusions and attacks related to various types of infrastructure and industrial control systems & SCADA networks.
9. Public engagement processes and mechanisms to measure citizen and business satisfaction or dissatisfaction with government services, finance and taxation policies.

There are companies that can carry out such surveys, help compile key datasets, analyze survey information and monitor huge amounts of data to look for trends and significant correlations that come from this big data, in some cases involving the processing of terabytes or even petabytes (i.e., a 1000 terabytes) of data to reveal or uncover key trends, reinforcing elements and relevant synergies. This type of searching of data can strengthen the planning and operation of smart city infrastructure.

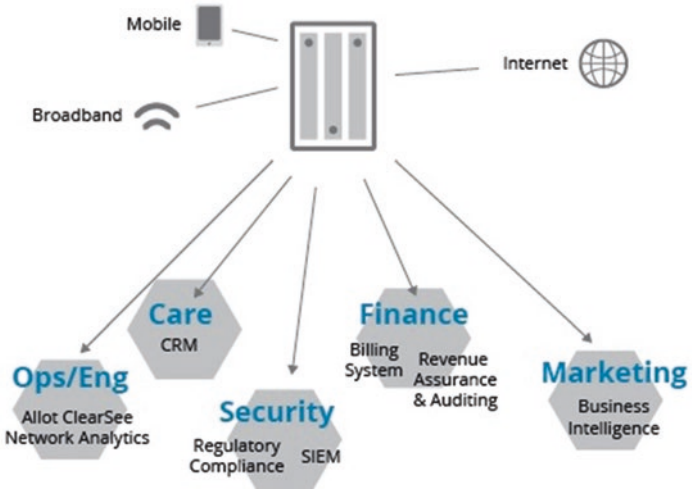

Fig. 13.2 This chart shows the various focus areas for big data analysis

According to a Datamation, which carried out a detailed analysis of big data analysis firms, there are at least 25 firms which their expert panel considered to be at the top of their game in this field. None of these firms offer exactly the same capability and analytic tools, each with areas of strengths and special capabilities. Below are these 25 firms engaged in the big data field, and this list is only the start of those engaged in this business. Table 13.1 represents the order of listing in the Datamation evaluation, but ordering is *not* in any way an indication of their ranked capability from 1 to 25. This is, in part, because these firms represent a diverse set of capabilities that focus on many different types of analyses.[3]

One can consult the details provided in this Datamation review to see a summary of the types of capabilities offered and the different types of analytical capabilities that are now available. These systems are typically able to cope with petabytes of data captured from mobile devices, broadband systems of various types such as LANS, Ethernet, satellite links, and Internet feeds can focus on the various functional areas indicated in Fig. 13.2 below.

The truth is that this is a highly volatile field with new companies popping up with new capabilities. Some of these new firms are small but highly capable. In some cases they provide smart models that can sample data from various sectors of a city's functional core to come up with what might be called smart data analysis. The small DataMi Corporation in Colorado was able to analyze declining patterns of use of public transportation in Orange County, California, and show how changing demographics were key. They were able to show that different age groups were meeting their transportation needs in different ways, with "Millennials" using ser-

[3] Andy Patrizio, "Big Data Companies," Datamation, July 14, 2017. https://www.datamation.com/big-data/big-data-companies.html.

vices such as Uber, Lyft and Car2Go. The DataMi model and smart data analysis was more dependent on an interactive system model of crucial urban drivers of change that was more important than churning through mountains of data.[4]

Part of the change in big data analysis is that new players are bringing new capabilities, such as the ability to process in real time data flows (i.e., Apache Spark capabilities) and also to process both structured and unstructured data from sources such as sensors equipped with Internet of Things connectivity. These new capabilities and new players can provide specialized vertical solutions rather than just general analytics.

This means that the volume of data processed is no longer the prime factor. Instead it is the variety of data that can be most important. Companies are thus now looking to integrate more varied data sources. This can be JSON to nested types in other databases to non-flat data formats. Sources, and connectors, are becoming more varied and crucial. A recent market analysis report by IDC has projected that worldwide revenues for big data and smart data business analytics will perhaps increase at a rate of over 12% year-over-year in 2017 to $150.8 billion. This same study projected that commercial purchases that include related hardware, software and supporting services could result in a compounded annual growth rate of about 12% through 2020.[5]

A large number of the big data analytics uses Hadoop. Hadoop is an open-source software framework for storing data and running applications on clusters of commodity hardware. It provides massive storage for any kind of data, enormous processing power and the ability to handle virtually limitless concurrent tasks or jobs. (See Fig. 13.2.)

Because of its distributed node configuration it is easily scalable to process higher volumes of data, and it can adjust to a node failure by shifting processing to other nodes. It has been used extensively to adjust to high volumes of data flows that come from data flowing from sensors and other sources emanating from IoT-connected units.[6] This can create valuable new sources of information, but also create potential sources of intrusion.

The purpose of such analysis is not only to find out past patterns and correlations that have occurred within a city and its operation. No, the key is to try to find trend lines and to see where more efficient design and potential synergies can make a city more efficient and its various functional parts to act less like silos and instead be more interactive.

---

[4] Interview with Stephan Andrade, CEO of DataMi Corporation, November 7, 2017.

[5] Andy Patrizio, Big Data Startups" Datamation, June 29, 2017 https://www.datamation.com/big-data/big-data-startups.html.

[6] "What is Hadoop?" SAS (accessed 7 Nov 2017.) https://www.sas.com/en_us/insights/big-data/hadoop.html#hadoopimportance.

Using New Urban Infrastructure Capabilities in Innovative Ways

The key to the future seems in part to hinge on finding innovative ways to use improved software or new hardware to accomplish new tasks, perform old tasks better or to protect infrastructure against intrusions and cyber-attack. In the simplest of terms it is a matter of rethinking how to use smart infrastructure to accomplish new tasks or make that infrastructure better protected from cyber-attacks. This can be best demonstrated by providing examples of how this has been accomplished in a variety of ways.

Arlington County in Virginia got a grant from the U. S. Department of Transportation to install a smart traffic signaling system across this small 24-square-mile (61.5 sq. km) county that is home to the Pentagon and other Department of Defense facilities, the Reagan National Airport, and many other key U. S. federal agencies. The main objective was to be able to change the traffic signals so that there could be a highly efficient mass evacuation of Washington, D. C. in case of a terrorist attack. This has resulted in the creation of a very high capacity fiber optic network that connects to key intersections across the county, but also connects to 100 sites, about half of these being schools and school facilities and half being county offices and facilities.

This system now has over 800 fiber strands installed and sufficient dark fiber capacity to support terabits per second throughput. The design allows sufficient broadband to support the county staff and official communication services and all networking capabilities, plus the broadband video conferencing and communications and IT networking needs of the schools. Additional dark fiber capability is now also being offered to U. S. governmental agencies, commercial organizations and universities. The design of the smart traffic signal system is such that first responders can, by using a special code, convert the traffic signal system on the Connect Arlington network into an emergency Wi-Fi network to support communications in the event of a major emergency in the vicinity. The system is also designed as a loop so that if the fiber cable system were to be cut it could still remain functional.

The key to a smart city and its effective design is to leverage the impact of smart infrastructures to have the maximum positive impact across as many sectors as possible. In the case of Connect Arlington this has been done in a variety of ways. The planned new wireless network for first responders that is being rolled out for the United States will use the Connect Arlington fiber network for back-haul connectivity among the six towers that will be needed to cover the entire countywide area. Connect Arlington can be used to support educational video links for the public school system, programming distribution for the local Arlington Independent Media (MIA) and video distributed courses for local universities. Connect Arlington will also provide back-haul connectivity for the various public Wi-Fi hotspots created at popular shopping malls, county governmental centers and libraries at multiple sites across the county.

Perhaps most relevant to this chapter the design of the system has also been conceived with cybersecurity in mind as well. The County 911 emergency response center is connected to a selected commercial carrier through two different switching centers as well as to Connect Arlington. Further there is a back-up center and a designated location at a fire station that is linked to Connect Arlington as well. The loop design would require the fiber network to be cut at two locations and there are two independent mobile command center vehicles (one for the police and another for firefighting and EMT services) that can link to both the Verizon and Comcast terrestrial networks at any location in the county. In addition the Arlington 911 center is directly linked to Fairfax County and over 20 other jurisdictions and the federal government.

These centers across the Washington, D. C., area are not only linked via dedicated communications systems, but there are also rehearsed emergency response plans that have been tested against full-scale simulations of attack or disaster events. These various disaster simulation scenarios include attacks on the metro rail system, a release of biohazards or lethal gases, either by terrorists or due to accident or natural disaster, and other possible cyber-attacks or physical assault events.

In addition to these fiber- and cable-based systems there will in time be the capability to provide broadband wireless service to police cars, fire trucks and EMT vehicles to aid with a variety of services related to criminal alerts and apprehensions and emergency situations. Satellite phones are also available in light of possible significant area-wide power failures. Leaky PABX systems are also deployed within the Metro-rail system to allow emergency wireless communications. County and school buildings are tested to insure the functioning of Wi-Fi and emergency wireless communications across Arlington County.

The Arlington County Department of Technology has the mandate to oversee the security of county SCADA and industrial control systems across water, sewage, electrical power, transportation systems, and other critical infrastructure. They also ensure that all high-rise buildings have functioning and resilient emergency communications capabilities. In areas with significant high-rise development, namely Rosslyn and Crystal City, there is a loud-speaker emergency address system in place to sound alerts where building structures might create dead spots for wireless communications access.[7]

Aircraft Cybersecurity and Smart Urban Infrastructure

Let's consider a totally different type of urban infrastructure and its security—that of aircraft cybersecurity. One might at first suggest that aircraft security against cyber-attacks is not even a part of the smart city and urban cyber-architecture. In truth, cybersecurity for aviation systems is very much a key element to be considered. Aircraft can be used to attack cities and nuclear power plants that supply vital

[7] Joseph N. Pelton and Indu Singh, *Digital Defense.*

electrical energy to cities. Further, aircraft are a vital part of most cities urban supply chain. Vehicles of all types are now increasingly dependent on sensors, cameras, digital processors and switches that are linked by the Internet of Things that relay vital data and information about their safe operation. A weakness in aircraft Traffic Collision Avoidance Systems (TCAS) or Automatic Dependent Surveillance-Broadcast (ADS-B) Systems can represent an opening for attack by cyber-criminals and techno-terrorists. In many instances the cybersecurity systems and software that can be created to protect aircraft can also be employed to protect automobiles, trucks, buses, mass-transit systems and rail systems.

At this time many aerospace companies are conducting research and design efforts to enhance and strengthen safeguards against cyber-attacks for civil and private aviation. Some efforts are seeking to provide real-time alerts to aircraft pilots if there are any warnings concerning attempts to launch a cyber-assault on a plane. These efforts are to some degree controversial.

Those engaged in developing alerts to pilots feel that monitoring communications to and from an aircraft and detecting "attempted or successful cyber intrusions" could prevent such assaults from actually resulting in airborne catastrophes. These advocates believe that aircraft could be equipped with artificial intelligence that could respond to such attacks successfully and avert air accidents. They further believe that this process would improve so-called situational awareness as to how to detect the nature, processes and perhaps even the identity or location of cyber-attack perpetrators.

Others argue that existing safety systems are effectively impenetrable from the outside and that all that is needed is better encryption, security keys, and end-to-end verification.[8]

This issue has become a sufficiently important area of debate that a bill has been introduced in the U. S. Congress that would mandate cybersecurity standards for commercial aircraft. In November 2017, Senators Bill Blumenthal and Ed Markey introduced a bill entitled the "Cybersecurity Standards for Aircraft to Improve Resilience Act (S. 679)" that will result in hearings on this subject. The object of this bill would be to mandate the creation of standards for air carriers to use to ensure against future aircraft attacks. Under the provisions of this bill there would be improved testing and maintenance of encryption and access systems, more security with regard to Wi-Fi access and enforced disclosure of intrusions and especially of any successful cyberattacks on aircraft systems. A similar bill is to be introduced in the U. S. House of Representatives.[9]

Nor is this just an area of concern in the United States. In June 2017 Major General Ansgar Rieks, head of the Germany Military Aviation authority, urged the adoption of a new research initiative within the German Ministry of Defense. This

[8] Aerospace Cybersecurity News, AIAA Data Service, July 2017. https://aiaa.informz.net/informz-dataservice/onlineversion/ind/bWFpbGluZ2luc3RhbmNlaWQ9Njc5ODc2NSZzdWJzY3JpYmVyaWQ9MTA2NDIyNzY4Ng==

[9] Senators Introduce Airplane Cybersecurity Bill, AIAA Data Service, Nov. 2017 Infor https://aiaa.informz.net/informzdataservice/onlineversion/ind/bWFpbGluZ2luc3RhbmNlaWQ9NjQ4MDM5OSZzdWJzY3JpYmVyaWQ9MTA2NTc4NzQ0OQ==

new effort would under Gen. Rieks direction would include new technical research projects and new and more highly encrypted and protective equipment to avert cyber-attacks on military aircraft, but presumably similar equipment could be used for commercial airplanes as well.

The government of Singapore in the summer of 2017 also reached a formal agreement with the International Civil Aviation Organization (ICAO) concerning security. The Singapore University of Technology has agreed to work with ICAO to develop a course on aviation security that is mainly focused on cybersecurity. Likewise, the Embry-Riddle Aeronautical University, which provides instruction programs in aviation and aerospace technologies on a global basis, has also recently developed a cybersecurity program for aviation and aerospace professionals. This aircraft cybersecurity program is available on campus and online, covering systems that are specific to the aviation security. It covers security measures specific to aircraft communications, tracking and positioning. This ERAU course covers Automatic Dependent Surveillance-Broadcast (ADS-B), Traffic-alert and Collision Avoidance Systems (TCAS), and Global Swim.

The Magnitude of the Challenge in Designing Smart City Infrastructure

Two case studies have been provided here. One was in the form of the nuts and bolts of how Arlington County has optimized the use of the smart infrastructure provided by the new Connect Arlington broadband fiber system to aid many key functions within the county. These applications are now being used to support traffic management, control and safety, emergency communications, video conferencing to enrich public education and public health, and provide free Wi-Fi service. At the same time the Department of Technology and IT Chief Information Security Officer are quite sensitive to the security of these new applications and the need to be cautious of attacks and the need for rapid switchover to back-up systems.

The second case study was in the form of providing better security and oversight to aviation that flies in and out of urban airports and are also a key part of the urban supply chain. The need to make all forms of aircraft safer against cyber-attacks has really only been clearly recognized within the last 3 years. The Malaysian airline Flight 370's mysterious disappearance in March 2014 started a widespread review of aircraft security procedures and processes.[10]

The point is that there is today an enormously broad range of flexibility, vision, foresight, and security concerns when it comes to the design, planning and operation of modern smart urban infrastructure. The areas of energy, communications and

[10] Sara Sidner, Catherine E. Shoichet and Evan Pere, Source: Flight 370's altitude dropped after sharp turn, CNN,

March 23, 2014, http://www.cnn.com/2014/03/23/world/asia/malaysia-airlines-plane/index.html

IT, and transportation are abundantly clear. But SCADA and industrial control systems for water and sewage systems, elevators, escalators, traffic signals, street lights, and the operation of the heating, ventilation and air conditioning systems in commercial and apartment buildings, hotels, malls and shopping centers, and essentially everything that makes a modern city work.

Guidelines for Future-Oriented Planning for the Smart City

The key elements that city planners, administrators and elected officials should make sure they use in future-oriented planning for the smart city include the following points: flexibility, vision, and foresight. Flexibility includes such concepts as modularity, diversity of applications and seeking ways to update infrastructure via software and multi-use processors rather than dedicated hardware. It especially means the avoidance of over-centralization and mega-density.

Vision entails a sense of what a city aspires to be, its mission and measureable goals and objectives for the future. Modern cities will likely use intelligent data analytics based on causal analysis and Bayesian diagrams of urban functionality to see what investments—capital and operational—are moving a city forward in the most effective and efficient manner toward its visionary aims.

Foresight is the most comprehensive planning aspect of all. Foresight means disciplined consideration of all of the critical what-if questions that guide wise and purposeful decisions and that look at costs when making future investments. It means examining whether intellectual infrastructure can replace or at least supplement physical infrastructure to make a city's operation more cost effective, more flexible, and more visionary in building toward longer term goals. Foresight is particularly key in terms of planning and executing digital security systems and also protecting against natural disasters, accidents and human error.

There are many things to be alert to with regard to the future-oriented planning of smart cities that should be constantly kept in mind. Is the design flexible enough to be reapplied to future uses and opportunities to serve populations decades into the future? If not, can a more modular, organic, or flexible software versus hardware design make it more flexible with a longer useful life? Can software upgrade capabilities avoid the need to deploy and replace physical hardware?

Each city is unique, and each city should obtain the expertise through staff and experienced contractors to develop longer-term improvement plans that are updated on a regular basis—typically 3–5 years. Nevertheless here are ten guidelines that a smart city might wish to follow in their future-oriented planning.

1. *Leverage the Flexibility of Software-Driven Gateway Access.* It is particularly relevant to consider new software gateway architecture standards that are designed to deliver a wide range of utility services on a flexible basis. Such gateway architecture can be used in the delivery, smart metering and upgrades with regard to electrical energy and renewable energy systems, broadband IT

services, telecommunications services of all types, including 5g mobile services, broadcasting and multi-casting services, water, sewage, and natural gas systems. It can avoid expensive black box upgrades and open up future opportunities. There are new intelligent gateway standards that allow many home, office, business and industrial systems to be updated via software and the use of multiple stand-by processors that can be activated rather than requiring the installation of a new black box or meter to be installed every time a utility upgrade is needed.

2. *Create Maintenance, Retrofit and Upgrade Schedules and Budgets for Financing Infrastructure Improvements and Modernization.* One of the 'unsmart' things that city governments can do is to neglect the need to maintain, retrofit and upgrade vital systems and infrastructure. This activity should be linked to longer-term financial planning. With prudent longer-term planning and budgeting for such maintenance, upgrades or retrofitting activity can be linked, perhaps performed in tandem, or even made part of longer-term capital financing and municipal bond programs. Capital financing on a longer-term bond financing can be carried out in tandem with 'pay-go' annual budgets to smooth the cost of these activities and avoid spikes in these costs on a year to year basis.

3. *Protect Vital Infrastructure by Creating Hardwire Command Access for Key Systems and Limiting Access by Units with Internet of Things Streaming.* There should be careful consideration about the hazards and potential pitfalls of allowing too much unfettered Internet interconnectivity, runaway access to critical infrastructure via the Internet of Things units, and strict guidelines concerning wireless access to critical control systems. There should be a technically knowledgeable IT governmental department within the city government that enforces this and rigor in the changing and use of passwords for SCADA systems, and command systems for vital infrastructure.
   Hardwire connectivity is often preferable to wireless systems that can be more easily accessed by hackers, but even wire, cable, and fiber-optic networks can be accessed with the right capabilities. Encrypted systems provide a degree of protection, but no system is failsafe. The key is to have vigilant experts monitor systems against intrusions and have a series of cybersecurity response capabilities at the ready and to plan strategies to localize the problem if there is an attack. There also need to be more "offensive" strategies to detect and prosecute cyber-intruders. Cybersecurity processes and agreements backed by ordinances, laws and even treaties or international agreements are needed to assist the effective enforcement of cybersecurity at the city, state, regional, national and international level.

4. *Cybersecurity and Emergency Readiness Review.* In short there needs to be a cybersecurity and emergency readiness review unit that is charged with urban risk minimization. Natural disasters, industrial accidents and training of personnel against erroneous commands needs to be a key part of this process that

reviews risk and risk prevention from a short, medium and longer-term perspective. If there is appropriate citizen expertise in these areas creation of one or more advisory commissions to address these issues would be an additional capability to create.

There are new opportunities that can come in such areas as the new cryptosystems, such as offered by blockchain ledger systems. These blockchain protective systems for vital data, voting information and financial transactions can better protect city vital records, improve the delivery of services such as paying of taxes and fines, and enhancing the speed with which building inspections are done or interactions with city staff and officials are completed. Cybersecurity and risk-minimization is part protection, but it also could be yet another opportunity for more efficient governmental services.

5. *Create within City Government a Longer-Term Planning Unit that Is Charged with 'Causal Analytics' and 'Intelligent Data' Review.* It is impossible to arrive at your desired destination until you know which direction you are driving in and if what you are doing is helping you stay on course. The current rage is big data analysis. This involves running large-scale datasets to see if you can pick out trends, and it can indeed be enlightening. But it is far more important to look at how a city government and community is structured and see if one can look at causal relationships to see which innovations and changes in policy, budget, technology or capital investments are creating the changes in actual results that a smart city is hoping to achieve against its longer term vision. Are job training programs resulting in new employment for residents as expected? Are more policemen, new emergency communications capabilities, or a smart network of security cameras better at enhancing urban security? Are telework systems able to enhance productivity? What programs are best at reducing a city's carbon footprint?

   Local political officials, government leaders, and planning staff often think they know the answers, but when they review the data in a systematic way they sometimes find out that assumptions, based on suppositions produce the wrong answers. Sometimes running datasets, and other times just surveying citizens, workmen and companies using tools now available on the Internet and social media produce a better feel for where things are going and what is working and what is not.

6. *Develop within this Longer Term Planning Unit the Ability to Review and Evaluate Disruptive Technology, New Public-Private Partnership, Reduce "Silos" Within a City Government and Let a Thousand Smart Systems Bloom.* Data analysis, causal analytics, citizen and business surveys and even management by objectives can help understand trend lines and provide an honest review of what is working and what is not. There is another side of the coin in future planning that allows one to explore new options and opportunities. Those that are pursuing a smart city approach are looking for innovations that can better city government, make it more responsive, more cost efficient and effective, enhance safety, and provide for key needs of citizens, residents and

businesses. One can set up convenient systems for people in a smart city to report on the location of potholes in roadways, burned out street lights, or even noise code violations.

The possibilities associated with new and sometimes disruptive technologies are almost endless. Self-driving cars, AI algorithms and increasingly capable robots will change not only our private and business lives but the nature of city government and how it delivers services to the public. Better sensors distributed in water mains, storm water systems, sewerage conduits, local streams and rivers, on tops of buildings or in utility systems can capture quickly and efficiently power outages during storms, increases in atmospheric and water pollution. Broadband mobile emergency communications systems, new mobile apps, and fiber-optic networks can enhance tele-education, tele-health services, snow removal, increase response times for fire, police and EMT first responders, and much more.

7. *Create Partnerships with Universities, Industry and Governmental Research Labs to Help Create the Next Generation of Urban Technologies and Systems.* Businesses and commerce are good at identifying new technology and services that respond to consumer demand and creating new markets. They are less adept at seeing how new technology might improve city governmental services or make urban governance more efficient. The developers of new photovoltaic systems are focused on developing solar cell systems that are more efficient in converting solar radiation into usable electrical energy, but not as adept at designing more resilient systems that might last three times longer. One of the key functions of a smart city could well be to identify the key new technologies, systems or even partnership arrangements between cities, industry and research labs to create new opportunities for city governments or households to use new technologies faster, more effectively, or at significantly lower cost. Sometimes the missing ingredients are more flexible financing arrangements, lifetime extensions for new or not fully proven new technology, zoning flexibility, or improved ease of installation. In such cases cooperative relationships between local governments, businesses and research institutes can create new institutional arrangements and/or new technologies or systems that help unlock the future more quickly and easily.

8. *Recognize the Importance of the Human-Machine Interface as the 'Singularity' Approaches.* In many ways the general citizenry is not equipped to cope with the speed of change that will come with living in a smart city as it unfolds in the next few decades. Ray Kurzweil, the artificial intelligence guru who invented the technology behind Siri, the knowledgeable lady that can answer almost any question that you might ask an I-Phone, has indicated that we can expect the singularity to come within the next two decades or so. Kurzweil envisions the singularity as the time in which smart robots with the reasoning ability of an average human being will be available to assist with labor and service jobs and a widespread number of tasks. He also envisions that AI will continue to become much more capable and help us innovate to create low-cost

sustainable energy, and an untold array of new technological capabilities.[11] Our friend and colleague Dr. Peter Diamandis, the creator of the X-Prize Foundation and one of the founders of the International Space University, describes this potentially awesome future as the age of Abundance.

Others such as Elon Musk and Stephan Hawking, however, have raised concerns about a future with the potentially runaway capabilities that come from an artificially high rate of intellectual evolution as holding risk for human civilization as we know it. What is clear is that the design of human-machine interface systems will be critical to the effective and safe operation of the smart city of tomorrow and that with the future prospect of the Internet of Everything, where most communications will be on a machine-to-machine basis, care must be taken. Control of vital infrastructure must remain linked to humans. Humans must stay in the loop with regard to the command and control of vital infrastructure.

The long and short of it is that AI and robots and ultimately the singularity provides a wide range of new opportunity, but human control and the ability to apply the brakes on runaway technology is a vital issue at the core of the smart city and its design and operation.

9. *Concentrate on Modularity, Eliminate Over-Centralization, and Encourage Individual Resilience and Environmental Responsiveness.* The concentration of people, resources and talent into cities has allowed innovation to blossom, research to expand and cultural, social and technical progress to be made. Today there are over two dozen megacities of over ten million people, and this trend is growing as more giant cities are created. This can result in overcrowded cities with a polluted atmosphere and waterways and significant vulnerabilities if supply chains are somehow disturbed or severe droughts experienced. There can also be transportation nightmares as a result of rush hour commuting, especially if some transport infrastructure fails. Further, real estate property values can become greatly distorted, and the creation of super skyscrapers of over 100 stories are starkly vulnerable to fire, earthquake, or terrorist attack.

   The core idea that we have proposed with regard to smart cities is that suburban sprawl is bad, urban density is good, but mega-density in cities can become bad again. Meta cities as satellites to core mega-cities can allow improved planning and technical innovation. This and other means of decentralization can allow efficiency of urban operation to be regained again.

   Even within mega-cities technological innovation and smart planning can allow for the avoidance of over centralization. District energy complexes supported by solar energy systems and renewable energy sources can become semi-independent and provide electrical power to the grid on an as-needed basis. Low-cost and broadband communications, via tele-work, tele-health, tele-education and other governmental tele-services can be substituted for transportation sys-

[11] Ray Kurzweil, *How to Create a Mind: The Secret of Human Thought Revealed* (2012) Viking Press, NY pp. 1–282.

tems and also aid efforts to reduce urban pollution and create a reduced carbon footprint. Modularity of design leveraged by use of software upgrades to replace the need for hardware retrofits can also be a part of this process that comes down to a philosophy as simple as avoiding putting all of one's eggs in a single basket. If these eggs can hatch into independent life-forms that can link together via broadband IT systems to provide mutual support and a new type of organic cooperation that is more efficient, more environmental sound, and less vulnerable to attack—then so much the better.

10. *Recognize the Central Importance of Environmental Sustainability, Demographics and Rates of Technological Innovation.* The effort at longer-term urban planning must always remain focused on the bigger picture and visionary goals. The increase of the global population from 800 million people in 1800 to 1.8 billion people in 1900, to some 7 billion people around 2000 has occurred in parallel with unprecedented technological progress. This rise of human population and modern technology has transformed the world as we know it. We have according to geologists now entered a new age where humans shape the fundamental geology of our times. This is known as the Anthropocene Age.

    Some believe that humans are transforming our planet, consuming its natural resources, and outstripping the ability of our finite 6-sextillion-ton planet to sustain future human populations of many as 12 billion people, 80% of which is living in cities by 2100. According to some environmental scientists, are on the verge of the sixth mass extinction that could rival the great K-T mass extinction that occurred about 65 million years ago with the mass 5-km disaster asteroid that wiped out the dinosaurs and led to the extinction of 75% or more of all species on Earth. In this Anthropocene extinction most large mammals and many other species of flora and fauna may be at risk if the number of humans and their patterns of consumption and pollution continue to grow apace.[12]

Smart cities must plan for a better future. This would be a future that is environmentally sustainable, based on more rational forms of consumption, communications and renewable energy. Ultimately this will require cities and the world to evolve toward a steady-state global population better suited to these future conditions and ultimate survival of the species. Meta-cities must not only be smart but also sustainable and optimized to a reasonable scale of efficiency. This will, in part, require the effective use of telecommunications and AI-enabled infrastructure to serve as a substitute for transportation and super-concentration of people in mega-city complexes.

---

[12] Jeffrey Kluger, "The Sixth Great Extinction is Underway – And We're to Blame," *Time Magazine,* April 24. 2018. http://time.com/3035872/sixth-great-extinction/ (last accessed April 2, 2018).

Conclusions

The complexity of modern urban infrastructure now frequently intersects with the most advanced digital processing systems and even more sophisticated software via machine-to-machine communications. The advent of Internet of Things that allows sensors, switches, back-up components and control systems to both "talk" and be "spoken to" provides enormous opportunity for more efficient and effective urban services. It also exposes smart city infrastructure to potential cyber-assaults by criminals, joy-ride hackers and in some instance techno-terrorists. It is important for all critical infrastructure to be actively managed and audited by well-trained cyber-security personnel, and particular attention needs to be paid to the interfaces and interconnection between and among these various systems.

A casino in the United States found that a smart system for controlling the filtering and temperature management of a large aquarium was used by hackers to access the financial records and credit card account numbers of the casino and its customers. The weakest link in a chain will break. The most unprotected and seemingly harmless part of an urban infrastructure, such as a smart drinking fountain with a processor to control the cooling of water might be the entry point for a hacker who is seeking to open a valve in a city's water supply to introduce a biohazard. The potential point of entry into a city's command and control system in today's ecosystem is difficult to anticipate. It can be a refrigerator, an incubator, or even an aquarium tank. This is now a serious concern, that a spurious cyber-command sent to a vehicle operating under autonomous control, or a hazard warning system in a plant producing noxious chemicals, could not only cause accidents but actually be lethal.[13]

Perhaps is important to realize that the smart city is highly dependent on technology and that if energy, communications and transportation systems are disabled and water and sewage systems cease to function, modern cities—especially megacities—can become death traps. Natural disasters, fires, cosmic hazards or assaults with bio-chemical weapons are hazards that must be recognized as a particular threat to large-scale urban centers. Planning of smart cities for the future must take into account these risks and ways to minimize those dangers.

If one looks beyond threats, the longer-term future can give rise to enormous new opportunities for smart cities as new technology, systems, and software can open up the possibility of more effective and cost-efficient health care services, low-cost continuing education and training, and neighborhoods better protected against fire, crime, and health emergencies. Governments can be more responsive to the needs of the citizenry and the process.

---

[13] Ellen Nakashima and Aaron Gregg, "On the lookout for malware that can kill" *Washington Post,* April 29, 2018, pp. G1 and G4.

Chapter 14
The Smart City: Build It and They Will Come

There are many terms that are being used today. Smart cities, Intelligent Community, smart planning, smart infrastructure, big data, intelligent data, broadband systems, digital defense and cybersecurity are just some of the phrases that are being used by journalists, urban planners and technologists. The result is that confusion abounds when it comes to the phrase smart cities. Does it mean better and more informed planning to make a city work more efficiently to make urban areas more livable and responsive to citizen needs? Or does it just mean using more automation, artificial intelligence and broadband digital networks to create smart infrastructure that operates more smoothly at lower cost?

The answer depends on who one talks to about what a smart city is and what it seeks to accomplish. Suppliers of digital equipment and software start by talking about what their technology can accomplish and how automation can save time, money, and labor costs and boost reliability and productivity. Their perspective might be described as technology push. City managers, mayors, city councils and urban planners start from the other perspective of 'better services pull.' In the best of circumstances there is a delicate balance between the technology push and the services pull. The main thing to note is that whatever approach is used to create a smart city, digital technology is only a part of the puzzle. Technology can create problems in the realm of cybersecurity. Misuse of technology can create problems larger than the issues and concerns they were first designed to address.

Whatever way one might want to define the smart city, digital destiny is its future. Citizens want to live and work in a city that provides higher quality of life, efficient government services, secure communities and the opportunity to prosper.

Any time one thinks about using technology to create a smart city there are number of concerns to be addressed and key questions that should be asked. Just a few of the most key questions include:

1. What are the longer term implications and will the use of new technology or automated systems be effective and responsive if the nature of the community and its demographics change?

© Springer International Publishing AG, part of Springer Nature 2019

J. N. Pelton, I. B. Singh, *Smart Cities of Today and Tomorrow*,
https://doi.org/10.1007/978-3-319-95822-4_14

2. What are the implications in terms of jobs, education, health care, tax base, social interaction, culture, and livability, housing, transportation, environmental sustainability, parks and recreation, safety and security, and so on? It is important to consider that improvements in one dimension may have negative implications in another dimension.
3. What is the longer term improvement plan and what investments, upgrades, and technology changes will contribute best to achieving overall goals? This implies an integrated approach to planning and overcoming the tendency for decisions to be compartmentalized and not consider "opportunity costs" that piecemeal decisions can imply.
4. How can planning and management be undertaken in more complete and effective ways other than just creating capital and operating budgets? This might be through such means as through the use of intelligent data, staff motivation, community involvement, public-private partnership, and other techniques.

The key to smart cities and smart planning is the ability to look at the big picture across all aspects of a community's needs now and into the future. This means looking at new solutions and their implications for potential change—both positive and negative. Improvements for one part of a city's population might hold negative implications for others. Thus it is particularly important to consider such important what-if questions and to evaluate the costs of making one decision in favor of another. A good solution might rule out an even better alternative decision that might ultimately produce even better longer-term results.

In this final chapter let's try to pull all the threads together from all the preceding text and consider what are the top "takeaways" that we hope readers will have gleaned from the earlier chapters.

Top Twelve Concepts Concerning How to Plan for and Implement a Smart City

Promote 'Service-Need' Pull and Avoid Technology Push

There is a classic issue with regard to the effective implementation of technology. This is the type of conundrum that decision-makers might face regardless of whether one is running a business, a benevolent organization, or a city or national government. Can new technology really help? Is it truly needed, or is it just a new toy that vendors want to sell?

In short are there actually problems, shortcomings, and substantive needs that technology can truly address to improve performance. A good application of technology is typically characterized as a "need" that pulls in new technology. This is starkly contrasted to a situation where technology is being "pushed" by suppliers where actual needs are vague or even non-existent. It is not enough for a new shiny

Fig. 14.1 A smart city must start with planning to meet longer-term needs

technology to seem neat. You, as a city planner, do not need to be the first kid on the block to have the newest toy. Stay away from "bleeding edge" technology that has not been proven to work and to solve problems.

Figure 14.1 below outlines how technology can provide help in improving safety, upgrading performance and reliability, cutting costs, and integrating disjointed and overlapping programs. In many cases the new technology might be to adopt a new process, create a new zoning tool, or reorganize the structure of government. However, technology is not a substitute for better management, improved longer-term planning, or organizational leadership.

This means that creating a true smart city does not require throwing a lot of technology into a city's infrastructure and automating all of a city's many functions. The place to start is by creating a comprehensive plan for improving an urban community to make it more livable and secure. It means striving to create an urban government that is more integrated, service-oriented and cost-effective. It means creating a longer-term city improvement plan that is viable across a spectrum of criteria that everyone supports. 'Everyone' here includes the broader community and its various components, the city's political leadership, the business community and the city's workforce. Everyone needs to be truly committed to achieving a common longer-term vision. Smart cities should be an equalizing force socially and economically.

Holistic Planning and Breaking Down "Silos"

The creation of a smart city takes both a broad and holistic vision of all the elements where improvement is being sought. The key is that it takes "the whole village" working together to achieve those goals. The enemy of a smart city is the division of a community into different 'silos' that divide a community and a city into different departments and creates separation instead. These divisions are frequently started by budgetary processes. Most annual budgets separate the various functions and facilities vital to a community into separate sectors of interest, and the allocation of financial resources are often viewed as a zero-sum-game. This serves to eliminate synergies and creates "budgetary silos" where units of government have difficulty of working together and sharing resources effectively.

It also requires a holistic view of the component parts that are needed to build a smart city over the longer term. Neither Rome nor a smart city can be built in a day. It took Copenhagen early a half century to create a city with a zero carbon footprint. Arlington County created a Long Term County Improvement Program in 1976–1977 that followed a consistent smart planning approach that has created a much improved community spirit, economically viable tax base, concentrated 85% of development on 15% of the land and led to broad recognition of the value of the so-called "Arlington Way." This, too, has taken over 40 years.

The key to a smart city is not budgetary management but creating a hierarchy of key steps that can be integrated together over the longer term. Each city has its own geographical location and ethnic, social and cultural makeup and its own economic and aspirational needs. Thus there is no one formula that covers the planning, operational and economic needs for all cities. The needs of a Lagos, Nigeria; a Mexico City; a Beijing, China; and a London, England, are clearly diverse and even wildly different. Nevertheless, the process outlined in Fig. 2.1 in this book is of value to all communities that aspire to be a smart city. This is so important that we have repeated these essential building blocks to creating a smart city again in this final chapter.

The key is creating a holistic longer-term vision of what the smart city aspires to be, which is supported by the entire community. This requires commitment for the longer term by the political leadership, the community, and the various departments and divisions of the government working toward that vision in a unified way for decades. Division within the community or within the city government or disagreement as to what the key goals are will eventually defeat a smart city initiative.

Political divides, conflict within various units of government or disputes between the business community and the citizenry will defeat smart city initiatives, and no amount of technology initiatives will be able to overcome such divides. The whole community and all of the governmental units must be working together, or rifts will defeat efforts to improve a city. Money, resources and business communities will go elsewhere. The five key building blocks to a successful 'smart city', as provided earlier, are provided yet again in this summary to emphasis their importance (See Fig. 14.2).

Leadership and visionary goals are important, but without community-wide buy-in these initiatives will ultimately fail. The whole community's buy-in and stakeholder's widespread support are the hallmarks of communities that have succeeded in creating smart cities.

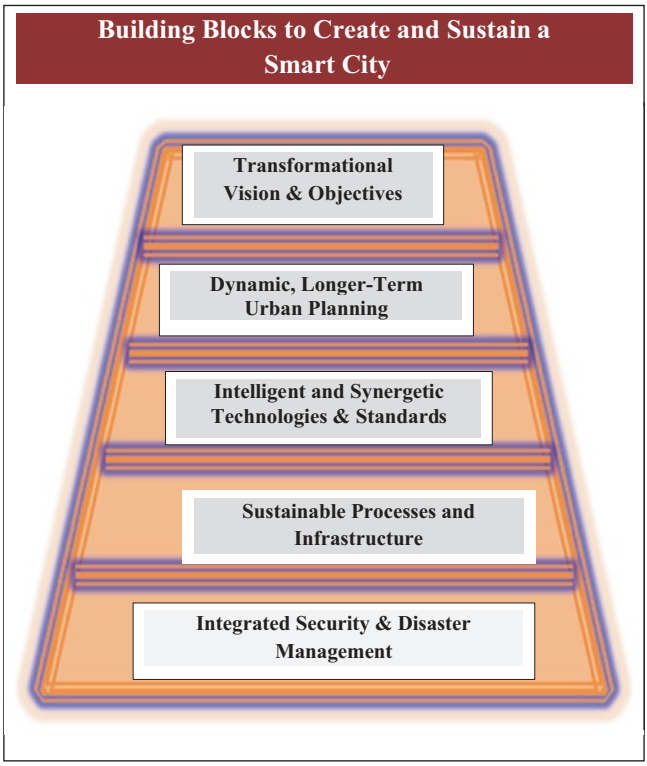

Fig. 14.2 To succeed smart cities must start with a holistic vision

Longer Term Goals Are Important to Progress

In many communities there will be an election, and new leadership will outline new goals and objectives for the future. This leads to new programs and perhaps the start of new activities in transportation, broadband communication systems, energy, education and health care, or some other type projects. In a couple of years, however, there might be another election and suddenly new priorities are established. This results in the previous programs being sidelined or canceled. It is only communities that create a broad consensus as to longer term goals and there is enough political stability and civic leadership as well as governmental commitment to these objectives for them to succeed.

Some projects, such as the transition from the use of traditional carbon-based energy systems to renewable energy sources or to create water desalination plants, to improve land use and the productivity of office buildings, hotels, shopping centers, schools and hospitals generally take a great deal of time. Other activities, such as new computer or broadband systems, or smarter street and road systems, can be accomplished much more quickly. The key here is actually the longer term, holistic goals for what a community wants to accomplish in reshaping its ultimate goals.

Some of the steps needed may take 1 or 2 years, others perhaps 3–5, and others perhaps decades to achieve.

The key to success is not how quickly upgrades or changes are accomplished. No, the key is to have an overall and integrated longer-term vision of what a city can and will be in a decade, two decades and a half century. This means knowing what land-use plans are desired. It means having plans for what the transportation, water, sewage, energy, environmental systems will look like years ahead. It means having clear-cut goals as to how educational and healthcare systems will best function in the future.

Annual budgets do not provide vision. Even five-year plans are insufficient. The idea is to create a broad consensus as to what the citizenry and business community needs are and how they will be met not next year but for the time when the sons and daughters of millennials are the leaders of tomorrow.

The Need to Adapt Constantly to Threats, Opportunities and New Technologies

Those who tend to discount longer-term visions of where a city will be some decades in the future note that conditions and circumstances constantly change. The reality is that we do live in a time of 'future compression,' where technology and artificial intelligence provide new capabilities it sometimes seems on a week to week basis. This just underscores the mistake of defining the future in terms of technology.

The key to longer-term planning is not to define future systems in terms like terabits/second or speeds of traffic flows. Technological rates of throughput are ephemeral. The goal should be to provide societal performance goals that are based on standards of living, education and healthcare, public and business confidence in governance of the community, viability of the tax base, balanced use of land, air and water resources, access to parks and recreational facilities, public safety and security, and sustainability of the environment. There are future-oriented goals such as creating a desirable urban environment that would draw future generations to return and live in their birth and schooling community. Another goal would be to create a community that is attractive to residents of all ages and of a balanced ethnic, social, economic and cultural background. The bottom line is that the smart city is defined by such societal performance goals, and the success in achieving these goals over time. Technology is a means to an end. It is never an end in itself.

The World Is Your Laboratory of Best Practices

To build a vibrant smart city a city must become a center of innovation. In the modern era, experimentation leads to successful implementation. Incubating and testing good ideas before implantation can increase the rate of success and mitigate risk.

City-states such as Singapore and Dubai, which are considered good examples of a smart city, spent decades designing, building and improving their smart cities.

There is indeed a danger in rushing into modernization and embracing what we referred to earlier as bleeding edge technologies. In the far past, experimentation was largely done in isolation, and the spread of new knowledge was often slow. In today's world it is possible to learn via the Internet and special interest groups exactly what new technology is available and how it fares in tests and trial implementations. The Intelligent Community Forum has now accumulated a database that documents the experiences of over 300 communities around the world in terms of their various experiences with not only various types of technology but new processes that can be applied to zoning, ordinances that allow—or ban—various practices, and a wide range of ways to make communities smarter, more competitive and responsive to the needs of businesses and urban citizenry.

The key point is that having a coherent and integrated long-range set of goals and objectives for a city is in no way in conflict with staying abreast of new technologies and innovative practices that can be adopted when proven to produce results. One can have long-term goals to improve transportation, the environment, education and health care, housing, and public safety and security while also, in the shorter term, adopting new technical approaches and new practices and processes along the way. The main thing is to do this with intelligence and reasonable caution.

Some cities may try a new water purification process and others might implement micro-generators in city streams to obtain low cost and clean energy. Yet others may create a tax benefit for building new structures or a new passive energy efficiency design. In today's world cities can experiment with new technology, tax incentives, zoning ordinances, or use of intelligent data analysis to make not only their cities smarter but provide information that can be shared with cities all over the world.

City leaders and planners must manage technological and societal changes proactively. For example, the growth of smart homes and smart offices now requires cities to reexamine their current policies and procedures governing such development. Similarly, fighting cyber crime and improving cybersecurity requires cities to reevaluate their data governance, staff training, risk mitigation plans, etc.

The point is that one of the great advantages of today's wired and wireless world is that experimental results as to things that work—and things that don't—can be shared around the world so that no city is forced to try innovations without useful and clearcut data to indicate which paths forward are most likely to work as well as where deadends also exist. A longer-term plan does not have to be static.

Active Citizen Participation, Public-Private Partnerships and Strong Commitment to Community Progress Are Essential

There have been grand experiments with regard to urban planning. In Brazil there is Brasilia. In Australia there is Canberra. In England there is Milton Keynes. In the United States the experiments have ranged over the centuries from Greenbelt to

Columbia in the state of Maryland. The Walt Disney Corporation has given us EPCOT, Centennial Village (an early smart city) and other visions of future living. For the most part these attempts have not been total successes, and often such experiments have provided insights into practices best to avoid as frequently as they have provided prototypes for the design and building of future cities.

It is not easy to get citizen and business input into a city's policy processes. One of the keys to success is to create a network of communities that feed their opinions and recommendations into the city's planning and decision-making process. The mechanisms can be advisory commissions to schools or city councils that cover a wide range of interests and disciplines. There can be committees of 100, neighborhood civic associations, civic federations, leadership training programs and extensive use of social media to get civic and business input.

This process is easiest with small communities, where town halls and personal interaction is easiest. As communities grow larger and more and more people live in rather anonymous high-rise apartments and condominiums, public input and involvement becomes more difficult. In regional urban complexes where there may be dozens or even over 20 different political sectors interacting, the ability to plan and interact effectively on a regional basis can become very difficult in terms of policy with regard to funding regional rapid transit or even agreeing on policies related to airport noise suppression.

One mechanism that can help get support for a number of civic improvement projects is the increasingly important mechanism of using public-private partnerships to finance new projects and to develop and implement new capital intensive improvements. However, these public-private partnerships must be transparent as to their planning, financing, and implementation to ensure that they are free of corruption and do not increase the cost of new services in an unreasonable or exorbitant way.

Continuously Measure Success and Identify Weaknesses

The best way to ensure that progress is being achieved with goals and objectives is to measure progress against milestones and reasonable indices of success. There is often a tendency to manage programs through finances and budgets. This translates into an index of success that can result in being able to spend the annual allocation of funds. Most budgetary allocations within a budget are typically decided as competitive exercises against other governmental departments. This means that management through budgetary oversight is not only ineffective, it is contrary to holistic thinking and interdepartmental synergies.

What is important in striving to achieve longer-term goals is the setting of clear objectives against measurable indices. The development of five- or even ten-year plans that involve cooperative relationships and smart city development goals that allow quantitative measurement represent a management by objectives system that can produce results and also engender cooperation. In an effective management by objective program there should be annual objectives, objectives against five-year plans and even

longer-term objectives that allow individuals, units of government, departmental managers and urban leaders to define what their mission is and how to work together to make their city smarter and better day by day, month by month, year by year and even decade by decade. A consistent longer-term vision is important, but a tangible and measurable system to chart progress toward such goals is also essential.

Monitor Technology and Automated Infrastructure to Assess Progress but Also to Identify Weaknesses

Technology progresses ever faster in the age of future compression. Improvements in computer systems and software, artificial intelligence, robotics and IT systems continue to move ahead apace. The adoption of consistent longer-term goals does not mean stagnation of technological advancement and upgrades to smart infrastructure and smart safety and security systems. Longer-term goals, as noted earlier, should be stated in qualitative ways with regard to livability, inclusiveness, growth of jobs and tax base, etc., and never in terms of technological performance. Technological advancement needs to be independently assessed as a means to an end. Technology advancement only makes sense if it can offer a better life for citizens, community sustainability and other smart objectives. Nevertheless technical advances need to be carefully monitored and understood.

This is not only in the context of better, faster, more reliable and safer and more secure, but also in terms of technological weaknesses. Many computer processing chips have recently been found to be vulnerable to cyber-attack. The design flaw was due to an attempt to increase efficiency by anticipating and executing commands before actually given. In late November 2017 a security advisory notice went out from Intel indicating "new vulnerabilities in the Management Engine (ME), as well as bugs in the remote server management tool Server Platform Services, and Intel's hardware authentication tool Trusted Execution Engine."[1]

This is but one of many examples of how well intentioned technical advancements can lead to security problems and flaws that can be exploited by cyber-criminals and techno-terrorists. There needs to be constant assessment of technology, not only in terms of potential advances of note but of security lapses and new types of vulnerabilities. Instant pay credit card systems seem quite convenient, for instance, but it is possible for cyber-criminals in close proximity to anyone without a protective covering of one's credit card to capture your information with a portable reader that can be purchased for only about $150.[2] City planners and management should think carefully of having a "white hat" team to explore new technical

[1] Lily Hay Newman, "Intel Chip Flaws Leaves Millions of Devices Exposed" Nov 30, 2017. https://www.wired.com/story/intel-management-engine-vulnerabilities-pcs-servers-iot/.

[2] Joseph N. Pelton and Indu Singh, *Digital Defense: A Cyber-Security Primer* (2016) Springer Press, Switzerland.

capabilities that might advance a smart city toward its goals, but also have a "black hat" team assess vulnerabilities and downsides to a technological advancement.

This team might also serve to provide a cautionary brake on using new technology. It might argue the case for others to test and prove new advances before committing a city to install systems that might become rapidly obsolete or prove vulnerable to attack.

Finally, it is key to remember that technological vulnerabilities do not hinge on cyber-attacks alone. Human error and especially natural disasters, from earthquakes and fires to solar storms such as coronal mass ejections, can serve to shut down power grids and take out supervisory control and data acquisition (SCADA) systems on which a growing number of cities depend. New developments such as the shift in Earth's magnetic poles that serves to lessen the natural protection that shields the world from damaging coronal mass ejections are just one of the dangers that city managers should be aware of and have defensive plans in place for.

Use Intelligent Data and Bayesian Causal Analysis to Make Better Investment Decisions

The usefulness of smart data is now widely known. Such analysis can find which factors and programs are most effective and pack the most bang for the buck. In the area of crime prevention and the most effective practices in coping with crime, such smart data analysis can help indicate which program or activity is best. It can help indicate which is the best way to spend resources, such as more patrolling policemen, more people with 911 alerts on their cell phones, or more effective video camera coverage. Smart data analysis should be a key component of a smart city and can help cities make better decisions.

The type of smart data analysis that has been carried out to date has largely been based on running large datasets in a nearly random manner to see if some sort of pattern or profile can emerge. There are new approaches that are based on causal models that can perhaps prove even more efficient. The idea is to create something called a Bayesian model of key functions within a city and posit the likelihood of various cause and effect relationships. The running of available datasets can help confirm the nature of those relationships and the degree of the likely impact. Further this type of intelligent data analysis that is based on demonstrated cause and effect relationships can also give rise to models that can help predict future relationships such as when the city's average age grows older or certain types of industries or companies are added or subtracted from the city's tax base and employment numbers. The point here is that analytic methods of this type can be expected to improve, and a smart city manager will find ways to continue to improve decision making and investment strategies for the future.

Trade-Off Analysis and Careful Consideration of Opportunity Costs Can Aid Decision Making

As a consequence of intelligent data analysis and other types of trade-off analysis one can hope to build toward more effective decision-making capabilities. This can serve to make limited resources and tax revenues to go farther and to have a more cost-effective impact. This type of trade-off assessment can help decide such issues and where and when and how public-private partnership might make sense. It can also mean that these types of consideration can help establish when automation and artificial intelligence might make sense and should be pursued and alternatively when a human workforce makes sense.

In considering trade-offs and 'opportunity costs' it is important to remember that cost-efficiency is only one index to consider. There are other key factors to be weighed, such as public safety, network security and reliability, back-up system capabilities in an emergency and flexibility to convert one type of service or capability to another in periods of crisis.

Part of this type of analysis should be finding new ways of performing tasks or offering urban services that are not merely 2% or 3% better. Rather a true smart city trade-off analysis should be using a process similar to that used by Google and ABC in trying to find breakthrough capabilities or alternative approaches that can be 30–50% better—not only in terms of costs but also in terms of effectiveness, safety, security or satisfaction among the citizenry or business community. The breakthrough is likely to be in the service sector such as education, healthcare, or crime prevention.

Cybersecurity Protections Are Increasingly Important

The world has changed more in the past three decades—essentially the time since the implementation of the Internet—than any other time in human history. It is said that it would be much easier for someone like Moses to come and live in the time of Thomas Jefferson, than someone who lived in the times of Thomas Jefferson to come and live in today's cyber-sophisticated world. Someone that does not know how to negotiate the world of cyberspace on a laptop or smart phone is lost in many parts of the world today.

Today's world is increasingly vulnerable to attack by cyber-criminals, hackers and even techno-terrorists. The extent to which one's banking accounts, local power supply, IT networks, water and sewage systems, various modes of transportation, and even electoral voting systems are now subject to cyber-attack is still not widely understood. Automation and use of artificial intelligence in private and public networks has made more and more people vulnerable to attack in more and more ways. Such attacks can be financial (i.e., wiped out savings or stock holdings at your bank or brokerage firm), can subject you to blackmail, loss of face, loss of reputation and standing in your community or the loss of your job or family (posting by trolls or

cyber-criminals of hurtful, salacious, or evidence of wrongdoing on social media or strategic websites that may or may not be true), or there could be a devastating attack on one's community. Such a techno-terrorist attack might be to send a command to a SCADA system to pump sewage into a water supply or to divert a railroad switch to send a train loaded with radioactive waste into another train loaded with passengers.

There needs to be more attention paid to backup security for cyber networks. These safeguards protect against techno-terrorist attacks that expose thousands of people to dangers. There need to be additional levels of protection on cyber-networks. These would be systems that would prevent, block or rescind spurious commands to disable the cooling system for a nuclear power plant, or to divert a train, or to poison a water supply, or otherwise launch a major act of terrorism against humanity. With more and more automation and use of artificial intelligence, the responsibility to design systems with a sophisticated protective human-machine-interface and loop delay review systems that prevent the worst of such attacks from occurring is becoming more critical every day.

Smart city development presents a significant opportunity for cities to prevent attacks and protect networks, IT systems and vital public data by integrating cyber defense with smart city architecture.

A recent meeting of the prestigious Institute of Computers and Communications (ICC) was devoted entirely to the subject of regulatory oversight and policy that might be needed with regard to automation and artificial intelligence. There is currently much debate, at least in the United States, about the need for more gun control regulation. The truth is that as important as the issue of gun control might be, the need for more effective control and regulation for computer and communications networks might be a thousand time greater in terms of people potentially at risk and in noting the probable danger of cyber-attack by a techno-terrorist.

A smart city has many dimensions, and we have tried to cover as many of them as possible in one fairly compact book. Is there a single magic formula that will make a city truly smart? No such silver bullet exists. But if there is one thing to keep in mind, it is that a city is created for people and not machines. If the people of the city are not involved in the decision-making and planning of what they want their city to be in the future, then this a true sign of failure. Citizen involvement is key. There might appear to be, at times, what seems to be too many citizen committees and advisory groups and networking processes. Citizen involvement might seem inefficient and time-consuming, but it is truly the most essential step in creating a smart city. Technology must always come second to what a committed citizenzy wants and needs to create a better future.

The Power of Automation and Artificial Intelligence Must Not Exceed the Limits of Effective Human–Machine Interfaces

This leads to the ultimate concern with regard to the design and operation of the so-called smart city. There is no doubt that automation and artificial intelligence can do so many tasks faster, more cost efficiently, and even with greater reliability, safety and security than humans when everything is working correctly. Self-driving

automobiles are ultimately expected to save billions of dollars and thousands of lives through the elimination of accidents. Yet there remains the concern that a hacker could use this same technology to create a runaway that could kill a captive driver.

Likewise a computer-controlled system could operate a metro or train system with greater safety than human operators, who can have a heart attack, be distracted, or simply make an error. Yet there is the concern that a computer program could also make a mistake or be affected by a coronal mass ejection (CME) that shuts down energy systems or some other AI or automated failure that cripple modern society as we now know it.

There continues to be a general concern that protective systems are needed against the future possibility of a destructive, self-aware artificial intelligence (AI) going amok. Not only are there many examples from fictional accounts, such as the computer envisioned in Arthur C. Clarke's name HAL 9000, or the Skynet computer that sends a cyborg to destroy Arnold Schwarzenegger in the *Terminator* movies. Key thinkers and scientists such as Stephen Hawking and Elon Musk have predicted this type of dilemma in future years. The over-reliance on automation and AI gives rise to concerns not only of computers and AI software making critical mistakes or wiping out a massive numbers of jobs but of running amuck as well.

Planning, designing and building a smart city is hard work. It is not something accomplished in a week, a month or even a year. Creating a smart city is a process that takes time and dedication that requires the commitment of many people that have a vision and are working with business and the entire citizenry to build a better tomorrow. It may be hard but it is definitely worth the effort.

Glossary of Terms and Acronyms

Adware This is one of the terms that is used in identifying pop-up ads that appear on your screen. These are usually enabled by installing freeware or shareware on your computer.

Android operating systems This is a Samsung developed operating signal and is the basis for developing applications for Android phones. These applications can reveal someone's user ID and potentially lead to other security breaches.

Antiphishing Software that aids in identifying and blocking on-line phishing activities.

Anti-virus Anti-virus software, which is often abbreviated as AV, is also sometimes known as anti-malware. Antivirus software was originally developed to detect and remove computer viruses, hence the name anti-virus.

API This acronym refers to application programming interface (API). Such an interface computer standard represents a set of routines, protocols and tools for building software applications. This is key in the use of the cloud or any other external computer resource. Of particular importance is whether the use is for one of the three types of usage within the cloud. These three types of usage are: (i) infrastructure as a service (IaaS); (ii) platform as a service (PaaS); or (iii) software as a service (SaaS). (Note: See the meaning of these terms as noted in the glossary elsewhere.) Many "free" API offerings, however, pay for their service by keeping track of users' patterns of use of the Internet or otherwise monitor user activities and sell this information. Thus 'free' services still come at a cost.

App A commonly used abbreviation for a computer application that might be installed on a computer or smart phone or other intelligent electronic device.

Apple Pay This is a proprietary system developed by Apple to allow instant payment via credit cards registered for this program and which uses near field communications (NFC).

APT Advanced persistent threat. These are threats posed by techno-terrorists or sophisticated cyber-criminals. These types of threats are the focus of the U. S. Cyber Command and other national attempts to defend against the most sophisticated of "black hat" hackers.

© Springer International Publishing AG, part of Springer Nature 2019

J. N. Pelton, I. B. Singh, *Smart Cities of Today and Tomorrow*,
https://doi.org/10.1007/978-3-319-95822-4

Automated bitcoin trading This is an automated program that presumably allows traders to use robotic trading capabilities in order to capitalize on bitcoin volatility with a variety of automated trading strategies that can allow leveraged gains to respond to increases or decreases in bitcoin valuation.

Back door This is a term used with regard to using root level machine instructions to access a computer. This can be accomplished by rootkits or other modes of attack via Trojan horse malware. Malware is often enabled by an attacker's ability to bypass normal authentication to gain access to a computer, electronic tablet or smart phone.

Backup memory One key form of protection of one's data files is to automatically back them up on ZIP memory sticks or have a protective service that automatically backs up one's files. Most corporations and governmental agencies have their files backed up at an offsite location to protect key files.

Bayesian analysis/Bayesian diagram This is a method of statistical inference that was initially developed by English mathematician Thomas Bayes. It describes a process that is frequently employed in causal analysis. A Bayesian diagram charts out key causal elements that interact with one another. This type of analysis allows statistical inference from historical datasets. A prior probability distribution for a parameter of interest is typically specified first and then tested against available datasets to obtain what is called a posterior probability distribution for the parameter or causal element being measured. The posterior distribution results provide the basis for statistical inferences and predictions of future likelihood of cause and effects. (Also see causal analysis.)

Big data This term refers to the processing and analysis of large amounts of data. Analytic algorithms operating on high speed super computers seek to find trends or revealed patterns that are helpful to analysts who are seeking new insights. The key descriptors of big data include the so-called 5Vs. These are volume, velocity, veracity, variety and value. This type of big data processing can be used in almost any context to reveal useful information that in some cases suggest changes in behavior or reveal flaws of various types. It can, for instance, be used to help athletes compete in competitions by revealing their strengths and weaknesses or those of an opponent based on the data from past performances. It can, in some cases, be used by urban planners to make more efficient use of public resources. There is in the modern world a prodigious amount of new information being continuously and instantaneously produced. As of December 2017 the following statistics on data use includes the following statistics on popular use of the Internet. Every minute, on average, 204 million emails are transmitted worldwide. In addition some 2.5 million pieces of content are shared on Facebook, 277,000 Tweets are tweeted, and 216,000 photos are posted to Instagram. (See also smart data.)

Bit This is the lowest element of data or information formed in a digital or binary system that refers to the distinction between either a "zero" or a "one." Eight bits of information are the equivalent of a byte.

Bitcoin A form of electronic money that allows the purchase of goods and services anonymously and that has the ability to increase—or decrease—in value. This

is known generically as crypto-currency. With this particular crypto-currency once one has installed a bitcoin wallet on a computer or mobile phone, it will automatically generate your first bitcoin address. You can create more bitcoin addresses whenever needed. You can disclose your addresses to your friends or retailers willing to trade in bitcoin. This is so you can make purchases or be paid in bitcoin. In fact, in many ways bitcoin operates very similarly to how email works, except that bitcoin addresses should only be used once for protective reasons. As of Dec. 2017 one bitcoin was valued at the equivalent of nearly $1800.00 (U.S). It is now publically traded, and traders are able to buy puts and calls to go long or short on the value of a bitcoin.

BitTorrent BitTorrent is a software company currently with the fastest torrent client "sync and share" software for Mac, Windows, Linux, iOS and Android.

Black hat This is the term that is given to someone who accesses a computer without authorization. This can often be for illegal gain or other unauthorized purposes.

Blockchain The blockchain process hides identities and can also be used to prevent a distributed denial of service (DDoS) attack as well as to facilitate a crypto-currency transaction. What is key to a crypto-currency transaction is called a blockchain ledger. This ledger helps to provide transparency for such transactions but also protect the identity of those engaged in the transaction. Although these types of transactions are in some ways anonymous, the blockchain ledger can link individuals and companies to crypto-currency purchases and ownership by allowing individual parties, called miners, to process payments and verify transactions. Rather than a central company presiding over the use of crypto-currencies, these blockchain originators serve central roles in the management and administration of this alternative currency system.

Blog This word was formed by putting together the words "web" and "log." A blog is any ongoing posting of information, news or personal information on the web for anyone to access.This is thus a web-based source of information about a person, an organization or an ongoing topic that can develop a group of followers and eventually evolve into a web-based magazine.

Bot This is a targeted computer or targeted processor (such as a device installed in an appliance) (see Internet of Things) that is taken over by a so-called bot-herder or zombie controller. Once a targeted machine is taken over by malware, the computer or processor can become a remotely controlled part of a botnet (also known as a zombie) that sends out spam or be used to engage in phishing or other remote illegal activities.

Bot-herder This is an informal slang term. It refers to a cracker or hacker that controls a botnet.

Botnet This involves a series of remote-controlled "bots" that can be used to send spam email or participate in distributed denial-of-service attacks by overloading a site that is thus being attacked. The word botnet is a combination of the words robot and network. The computers that form a botnet can be programmed to redirect transmissions to a specific computer, such as a website that can be closed

down by having to handle too much traffic, called a distributed denial-of-service (DDoS) attack—or, in the case of spam distribution send a message to many computers.

Broadcast services This is a term defined by the International Telecommunication Union (ITU) that refers to direct broadcast services by satellite to individual users. See also direct broadcast services.

BYOD Bring your own device. Many organizations are allowing employees to bring their own device to work, which can create a variety of vulnerabilities. In telework environments when employees are working from home with their own equipment, this may involve unsecured wireless local area networks, which can allow unauthorized access to enterprise networks.

Causal analytics This is a type of analysis that seeks to chart functional cause and effect relationships, often using a Bayesian diagram to indicate anticipated relationships that can then be determined using relevant datasets to reveal the nature and degree to which these causal relationships actually exist. This technique can be used within any interactive system but is particularly relevant in analyzing causal relations within a town, city or political, social or economic entity. Use of big data analysis in this context is sometimes referred to as intelligent data analytics.

CAT The causal analytics toolkit (CAT) is an Excel add-in for Microsoft Windows users. This tool can be used to assist with causal analytics. CAT was initially developed by Cox Associates with support from a number of different academic organizations. Due to the risks, expense and realities of introducing new software products, Cox Associates made the decision not to take CAT to market as a general purpose causal analytics product. Rather, a targeted industry solution approach was chosen, to be implemented through DataMi LLC, of which Cox Associates has 32% ownership.

Circular economy/Creative economy/Sharing economy The latest concepts related to the design of a smart city center not only on the use of technology but also on economic concepts centered on co-creation and moving beyond a strictly linear economy. A circular economy is thus focused on co-creation or a regenerative system. This emphasizes limiting new resource input and all forms of waste, energy leakage and polluting emissions. Such a circular economy with a smart city can be achieved through long-lasting design, maintenance, repair, reuse, remanufacturing, refurbishing and recycling. This is in contrast to a linear economy that can lead to increasing rates of consumption and pollution. A linear economy is sometimes referred to as being based on a 'take, make, and dispose' model of production.

Click fraud Click fraud is the method of generating inflated numbers as to traffic on a commercial website. This is particularly the case where ad viewings are tied to payments for online ads. The fraudulent viewings are either using non-human sources—such as lines of code that automatically click on brands' ads—or hiring a number of users to manually click on the same ads in order to increase the amount of revenues tied to ad viewings.

CME Coronal mass ejection (CME). This is a particular type of solar storm that involves an ejection of ions from the corona of the Sun. It is usually in conjunction

with a solar flare of intense radiation. A CME, if it strikes Earth, can do major harm to pipelines, the electronic grid and also satellites and other electronic devices.

CONTU This was the U. S. Commission on New Technological Uses of Copyrighted Works that ruled which computer programs could be protected as copyrighted works. (See Copyright of computer programs and their legal status.)

Cookie Cookies are small files that are specific to a particular computer and website. They allow the server to deliver a page tailored to a particular user. In order to find out whether your browser allows your "cookie" to be captured you need to go to the "cookie checker." Many websites do not allow access unless they are able to capture this specific file information.

Copyright This is a protective right that is granted to developers of new computer programs and to writers of books and published articles. It allows copyright holders of computer programs to license the use of and derive profits for such copyright-protected materials. "Copyleft" as opposed to "copyright" says that anything taken for free and modified must in turn be distributed for free.

Copyright of computer programs and their legal status In 1974, the U. S. Commission on New Technological Uses of Copyrighted Works (CONTU) decided that "computer programs, to the extent that they embody an author's original creation, are subject matter that have the right to be copyrighted." CONTU also decided that software and its source code were not copyrightable and thus this constituted public domain software. This is currently a matter of legal dispute in a suit involving the Electronic Freedom Foundation and the SAS Institute. The 1983 Apple v. Franklin decision and associated legislation clarified the status for "object code" in specifying that the Copyright Act gave computer programs the same copyright status as literary works. In 1999, in the U. S. court case Bernstein v. United States ruled that source code should be considered a constitutionally protected form of free speech. Proponents of free speech argued that because source code conveys information to programmers, because it is written in a language, and because it could be considered an artistic form of expression, it is accordingly a protected form of communication.

Cover through complexity attack This is an attack that creates diversionary data or noise in a network to create a cover to disguise the actual attack on a computer or network.

Cracker A cracker (also known as a black hat hacker) is an individual who seeks to bypass Internet security or gain access to other people's or organization's computer networks. The general view is that, while hackers build things, crackers break things. Cracker is the name given to hackers who break into computers for criminal gain, whereas hackers can also be Internet security experts hired to find vulnerabilities in systems.

Crypto-currencies This are forms of electronic money that are encrypted so that their source is protected and is not tied to a particular national currency. The better known crypto currencies are bitcoin, Ethereum, Litecoin, Dogecoin, Ripple, Monero, Dash, Stellare Lumens and Xem. These are in many cases traded on exchanges so that the value can increase and they can be sold both long and short.

Cyber-attack There are number of different strategies for a so-called stealth cyber-attack on a network user. These strategies include: (i) detection evasion; (ii) targeting; (iii) dormancy; (iv) complexity; and (v) persistency. The most common such attacks typically seek to evade the security system used on a network or an individual computer. The attacker bypasses the operating system by seeking to avoid the anti-malware and other security software.

Cryptowall 2.0, 3.0 and 4.0 The CryptoWall is a ransomware Trojan that carries the same strategy as a number of other encryption ransomware infections such as Cryptorbit or CryptoLocker. The CryptoWall is designed to infect all versions of Windows, including Windows XP, Windows Vista, Windows 7 and Windows 8. As soon as CryptoWall infects a computer, the ransomware uses the RSA2048 encryption to encrypt crucial files. Effectively, CryptoWall prevents computer users from accessing their data, which will be encrypted and out of reach. Typically users of infected computers are asked to pay $500 to obtain the decryption software to unlock their computer. Cryptowall 4.0 is the latest version.

Cybersecurity A number of methods and tools that can be used to protect one's online privacy or prevent or avert digital attacks on one's computer, smart phone or other electronic devices via various types of malware.

Dark net This is an encrypted website that allows anonymous access. It was established to allow citizens in dictatorships to be able to communicate openly in order to avoid detection. It has over time evolved as a means to communicate anonymously within the Internet without identification and is, in this regard, now being used by cyber criminals and techno-terrorists for many types of illicit activities.

Darwin Darwin is an open-source Unix operating system released by Apple Inc. in 2000. It is composed of code developed by Apple, as well as code derived from NeXTSTEP, BSD, Mach and other free software projects.

Data bomb or logic bomb A data bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger) if the programmer is terminated from the company. Software that is inherently malicious, such as viruses and worms, often contain data bombs that activate a certain payload at a pre-defined time or when some other condition is met.

Data haven A data havens operates in many ways similarly to what are also called tax havens, or corporate havens. These are locations that serve as a refuge for uninterrupted or unregulated data. Data havens are locations with legal environments that are friendly to or protective of allowing computer networks to be free from governmental inspection or intrusions. Thus data havens offer protection of enterprise networks and data centers' content and associated information. Tor's onion space (i.e., a hidden service), Haven Co (centralized protected data haven), and Freenet (decentralized data haven) represent three relatively well defined models of virtual data havens that are currently in common use. Countries that provide favorable tax laws to shelter income also tend to have laws to protect secure data storage. Some of these countries include the following. There are a number of law firms that specialize in advising on setting up accounts in tax haven/data haven countries.

Table of countries listed on various tax haven lists	
Caribbean/West Indies	Anguilla, Antigua and Barbuda, Aruba, Bahamas, Barbados, British Virgin Islands, Cayman Islands, Dominica, Grenada, Montserrat, a Netherlands Antilles, St. Kitts and Nevis, St. Lucia, St. Vincent and Grenadines, Turks and Caicos, U. S. Virgin Islands
Central America	Belize, Costa Rica, Panama
Coast of East Asia	Hong Kong, Macau, and Singapore
Europe/Mediterranean	Andorra, Channel Islands (Guernsey and Jersey), Cyprus, Gibraltar, Isle of Man, Ireland, Liechtenstein, Luxembourg, Malta, Monaco, San Marino, and Switzerland
Indian Ocean	Maldives, Mauritius, Seychelles
Middle East	Bahrain, Jordan, and Lebanon
North Atlantic	Bermuda
Pacific, South Pacific	Cook Islands, Marshall Islands, Samoa, Nauru, Niue, Tonga, Vanuatu
West Africa	Liberia

Source: https://fas.org/sgp/crs/misc/R40623.pdf

DDoS This is a distributed denial-of-service (DDoS) attack, such as SYN-flood, Get-flood, or Post Flood attack. This type of attack is usually achieved via a "botnet."

Deep Net or Deep Web This is sometimes also called the hidden web or invisible web. The deep web is the opposite of the "surface web," whose contents can be accessed through search engines**.** This 'deep net' allows the interconnection of all the many thousands of component webs that make up the Internet and facilitates the overall functioning of this worldwide network of digital systems. It should be distinguished from the "dark web" that operates within the deep net or deep web. This dark web avoids detection by search engines largely in order to carry out criminal, terrorist or surreptitious activities.

Defense-in-depth (DiD) This the traditional approach to digital data protection that uses a series of layered protective systems.

Demographics This is the study of population characteristics for countries and regions and how these characteristics change over time with respect to family size, health and death rates, and age distribution.

Detection evasion This type of cyber-attack seeks to evade the security system used on your network and individual computer. The attacker typically moves the root level and bypasses the operating system in seeking to avoid the anti-malware and other security software.

DHS Department of Homeland Security.

Digital encoding or encryption This is a much more secure form of encoding of a signal that would require a computer processor a considerable time to ever decode. If the key to decode a digital signal were sufficiently complex, such as a 62-bit or 128-bit code, then it would be virtually impossible to decode without knowledge of the precise code.

Direct broadcast service This is a satellite service where either radio, television, streaming services or download of digital applications are sent directly to consumers' homes or offices via a satellite dish and is a competitive service to cable television services.

DNS Domain name system. (See Phishing and Pharming on how this system can be abused by a black hat hacker.)

Dogecoin A crypto-currency.

Domain name system (DNS) server in computer networking The DNS is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network using the Internet Protocol. The key function of the DNS server is to translate a specific domain name assigned to each of the participating entities. Most prominently, it translates domain names, which can be easily memorized by humans, to the numerical IP addresses needed for the purpose of computer services and devices worldwide. The domain name system is an essential component of the functionality of most Internet services.

Dormancy This is when an attacker typically plants a "dormant" malware (Trojan horse or time bomb) that waits for a later time to mount an attack.

Dual use satellite service This refers commercial satellite systems that also provide military or defense-related services. Significant dual use of commercial satellite systems is now common around the world. Satellite systems with significant such use include Intelsat, Inmarsat, Eutelsat and Telesat, among other systems that provide this type of access.

Einstein 3 This system draws on commercial information technology and specialized government technology to protect the U.S. government data networks. It conducts real-time full packet inspection and threat-based decision-making on network traffic entering or leaving executive branch networks. Einstein 3 is deploying and testing intrusion prevention systems across the federal government offices. It is hoped that EINSTEIN 3 will assist the Department of Homeland Security (DHS) in defending, protecting and reducing vulnerabilities on federal executive branch networks and systems using a system known as US-CERT.

Electronic Freedom Foundation This is an independent non-governmental organization based in San Francisco. It is dedicated to the defense of "electronic freedom" on the Internet. The main objective is to defend the rights of individual users of the Internet to be free from intrusive governmental monitoring and surveillance. It also champions the idea of computer software interoperability and actively resists the initiatives to extend copyright protection to prevent reverse engineering of software to maintain interoperability. (See SAS Institute.)

Electronic village This is the concept of the world being closely connected via electronic media as first presented by Prof. Marshall McLuhan in his writings.

EMP Electromagnetic pulse. This can be generated by an atmospheric explosion of a nuclear device or by a solar storm in the form of a coronal mass ejection (CME).

EMV chip This is a chip inserted in a credit card that prevents counterfeiting and fraudulent use of credit cards. Counterfeiting is much easier to accomplish if the

counterfeiting organization only has to embed your credit card number on to a magnetic strip. EMV stands for "Europay, MasterCard and Visa" that pioneered the development of this chip. (See also smart chip.)

Fig. G.1 An example of a credit card with an embedded EMV chip

Encryption This means to code information to protect it being read or accessed by anyone except the intended reader. Decryption is the process of decoding the message with a decryption key so that it can be read.
ENISA European Union Agency for Network and Information Security, which is headquartered in Crete, Greece.
Etherium A crypto-currency that is second in size to bitcoin.
Exabyte This is a term that refers to a million terabytes of information or a million trillion bytes of information or a thousand petabytes of information.
Fake news This is information that is made up and often distributed via social media and sometimes political leaders in order to create political spin or influence public opinion or elections or influence the opinions of followers.
Faraday cage This is a grid around an electronic device or system that prevents radiation from penetrating within the cage to extract information or disable the device. This is named after the famous physicist and theoretician Michael Faraday.
Firewall This is a network security system that controls the incoming and outgoing network traffic in order to protect the internal network against spam and malware such as worms, viruses, zip and logic bombs and Trojan horses. A firewall is based on a set of rules that isolates and protects the internal network from harmful software and cyber-attacks. A firewall thus establishes a barrier between a trusted, secure internal network and another network (e.g., typically the Internet) that might potentially be a source of malware of various types. This can be used at varying degrees of sophistication within a home-based network, a small office, or an entire corporate enterprise network.
FISMA Federal Information Security Management Act of 2002.
5G Fifth-generation mobile services. This is latest in broadband mobile cellular services that support video streaming and other higher throughput mobile services via smart phones.
Fixed-function appliances These are protective systems for data networks with a fixed function to prevent unwarranted intrusions. These begin with a firewall and include a number of other protective functions.

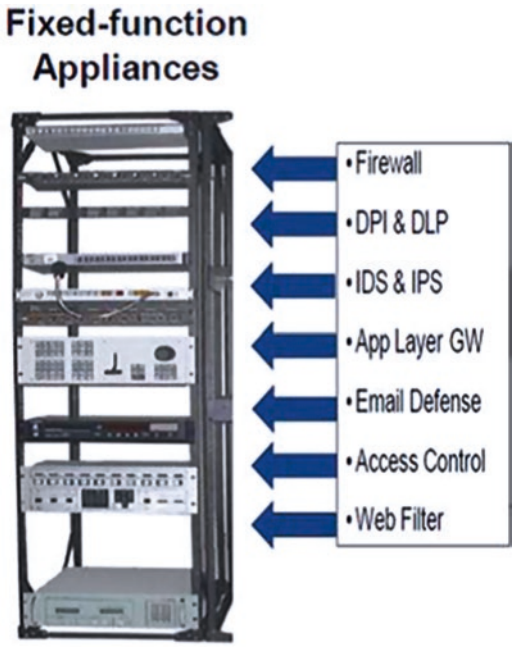

Fig. G.2 Diagram of a fixed functional appliance for digital security

4G-LTE 4th generation mobile satellite services—Long Term Evolution. Much of the LTE standard addresses the upgrading of 3G UMTS to what will eventually be 4G mobile communications technology. A large amount of the work is aimed at simplifying the architecture of the system, as it transitions from the existing UMTS circuit + packet switching combined network to an all-IP flat architecture system.

Freenet Freenet is a peer-to-peer platform for censorship-resistant communication. It uses a decentralized distributed data store to keep and deliver information, and has a suite of free software for publishing and communicating on the web without fear of censorship.

Free Software Foundation This foundation is a 501(c)(3) non-profit organization. It was founded by Richard Stallman in 1985 to support the free software movement. The basic principle of the foundation is to promote a worldwide universal freedom to study, distribute, create and modify computer software, with the organization's preference for software being distributed under copyleft ("share alike") terms. It promotes the use of its specifically developed GNU general public license. The FSF was incorporated in Massachusetts, where it is also based. From its founding until the mid-1990s, FSF's funds were mostly used to employ software developers to write free software for the GNU project.

Freeware This is software that is available under general public licensing without royalty.

GIF Graphic Interchange Format that is extensively used on the world wide web.
GIS This acronym stands for Global Information System. It can refer to any information system that attempts to deliver the totality of measurable data worldwide obtained most typically by remote sensing devices and formatted for easy access as to its exact geographic context and in an exact location defined in an X, Y and Z axis. It can be effectively used for urban planning and zoning, for providing first responders with exact locations to respond to emergency calls and many other practical uses.
GNU General Not Unix (GNU) General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. It promotes the concepts of "copyleft" or "share alike" as it applies to new programs that are developed on this free use basis such as Linux-based software.
GSM Global System for Mobile Communication, or Groupe Special Mobile, was a digital cellular service standard first developed in France and elsewhere in Europe. This is now being phased out and replaced by 4G broadband services.
GUI Graphical User Interface, a GUI (pronounced as either G-U-I or gooey) allows the use of icons or other visual indicators to interact with electronic devices, rather than using only text via the command line. A GUI uses windows, icons and menus to carry out commands, such as opening, deleting and moving files. One of the vulnerabilities of mobile devices is related to the graphical user interface that could be tricked into hiding a security dialog.
Hacker This is term that refers to those with extensive computer science or a system analysis background and is not necessarily a pejorative term. So-called "black hat hackers" or "crackers" use their knowledge and skills to break into computer networks for illegal gain or other purposes against the interests of the user community.
Hacktivists This is a term that is applied to those that hack into computer networks to obtain and reveal information that they feel is being withheld from the public and that it is worth the risk of undertaking a network incursion to reveal this information. Wikileaks is perhaps the prime example of what might be called a hacktivist site. Edward Snowden is in under U. S. federal indictment for the release of classified information that he obtained illegally from National Security Agency computer files. He has also claimed that this was the purpose of his activities.
Hadoop Hadoop is an open-source software framework for storing data and running applications on clusters of commodity hardware. It provides massive storage for any kind of data, enormous processing power and the ability to handle virtually limitless concurrent tasks or jobs. Because of its distributed node configuration it is easily scalable to increase higher volumes of data processing, and it can adjust to a node failure by shifting processing to other nodes. It has been used extensively to adjust to high volumes of data flows that come from sensors and other sources such as IoT-connected units. It was released by Yahoo as open source software in 2007. The management of the software and its updates is provided by the Apache Software Foundation.

HAPS High Altitude Platform Systems.
HMI Human-machine interface (HMI) station. This is the display station that provides vital information to the operators of Supervisory Control and Data Acquisition (SCADA) networks. It alerts human operators as to the need for responses to signals indicating errors or a need for corrective answers, repairs or other responses. Although there are algorithms that can be developed to respond automatically to most of the various errors and problems, it is important to always have human operators in the loop.
HTML The HyperText Markup Language.
HTTP The HyperText Transfer Protocol.
HTTPS HyperText Transfer Protocol Secure. Technically, HTTPS is not a protocol in itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.
Hyperlink This is a link between one node in the world wide web to another and is often used to cross reference an online book or instantly move to a site to obtain pertinent cross referenced information.
IaaS Infrastructure as a Service. This is a term used in the provision of various types of services from the cloud. Infrastructure as a service (IaaS) typically offers various types of information technology operations. There are often what are typically called "fully managed" IaaS types of offerings that can be used to develop applications and run production-ready workloads or so-called "soft layer" IaaS offerings that involve less expense and a lower level of support. See also Platform as a Service (PAAS) and Software as a Service (SAAS).
Identity theft This is the stealing of one's identity usually for the purpose of illegal gain. Identity theft can be accomplished through physical means such as robbery or obtaining discarded records. In today's cyber world, the usual means of identity theft is through hacking into someone's computer and obtaining personal identifiers such as social security numbers, banking and brokerage accounts and associated access codes or personal identification numbers. Identity theft can also be used to create an alternative identity under which name a crime or even an act of terrorism might be conducted. Thus protection of a personal identity is crucial in a world in which financial and business activities are increasingly electronic.
IEEE Institution of Electronics and Electrical Engineers. This large professional organization also develops standards. Its standard for Wi-Fi wireless networks, namely 802.11 in its various forms, is key to the provision of wireless access services.
IETF Internet Engineering Task Force. The standards coordinating body for the developing of Internet related protocols. The IETF sends out RFCs (recommendations for comment) to seek to coordinate and reach agreement on various protocols and standards of use.
Insider Threat Consideration of insiders obtaining information that is inappropriate is the focus of many new initiatives to protect data networks and databases. The traditional approach is to assume that everyone that can access a layer is not a

threat to a database. But more recently there has been a concern with operations or activities carried out once a database has been accessed. To some extent this is a reaction to the notorious case of Edward Snowden's clandestine obtaining of information from the National Security Agency (NSA). These procedures are geared to analyzing whether activities carried out by someone within the system, and perhaps particularly within a cloud environment, might result in someone obtaining information that is actually inappropriate. The chart below illustrates within the U. S. NIST's layered framework points where a user might have access but nevertheless carries out inappropriate taking of information.

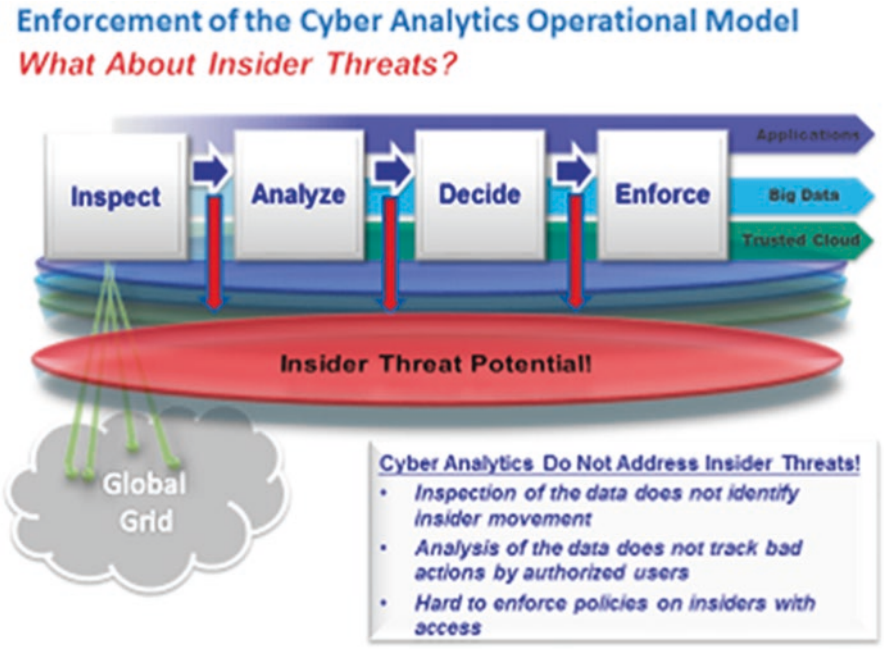

Fig. G.3 U. S. National Institute of Standards and Technology (NIST) diagram of insider threat potential for data networks

Intelligent Community Forum This is an organization headquartered in New York City that hosts an annual conference, sponsors a number of online training courses and sponsors a global competition to select top performing intelligent communities from around the world. The selection process conducted by a large number of international judges is based on a wide-ranging set of criteria related to broadband telecommunications, automation, IT systems, as well as education, healthcare and community involvement criteria. It also hosts a large database of best practices that have been collected and stored electronically in a computer accessible network and allows access to this information that was compiled from over 300 communities worldwide.

Intelligent Data This is a term that is used to describe qualified and authenticated data that is used to test causal analysis models to determine if certain patterns of cause and affect can be verified and the degree to which such causation exists. See CAT.

International Telecommunication Union This is the U. N. specialized agency that is formally assigned responsibility for creating global standards and protective systems for telecommunications and information networking as well as the allotment of radio frequency spectrum and the prevention of jamming and electromagnetic interference of telecommunications and information networks.

Internet This is the interlinked worldwide network of thousands of digital networks that are linked together by the Internet Protocol.

Internet of Everything This is a new term that refers to the use of IoT technology and cyber-systems in virtually all aspects of modern society and impact of automation and the growing pervasiveness of machine-to-machine (M2M) communications and automated systems, including the cybersecurity risks that are involved.

Internet of Things The latest trend is to make all sorts of appliances, machines and electronic devices (such as refrigerators, washing machines, security systems, automobiles, boats, buses, etc.) smart to the extent that they contain digital processors and the ability to communicate via the Internet. This means that so-called botnets that can engage in such activities as distributed denial of service (DDoS) can in the world of Internet of Things come from literally billions of these smart devices.

Intranet This is a private and typically password-protected dedicated network set up by a company, an office or an organization, or even within a home. It can be either a wired or wireless digital network and is usually protected by an antivirus, firewall or other security measure. This can be as large as a worldwide access network (WAN) or an enterprise network for a very large corporation. It can also be a municipal access network (MAN) operating within a city, or a local access network (LAN) that is geographically limited even within a single household.

Intrusion An intrusion is a penetration of a firewall or other protective measures that shields a site from unauthorized entry. Under legislation that has been enacted in a number of countries including the United States many critical infrastructure utilities and public governmental bodies websites, especially for financial institutions such as the Federal Reserve, Security and Exchange Commission who oversee stock markets and commodity exchanges, etc., are required by law to formally report on intrusions and the details by which such intrusions were made. This process has been put in place to establish the level of vulnerability that exists, the nature of such attacks, and protective measures that can be implemented to prevent future attacks.

iOS This is the operating system for the I-Phone, the I-Pad and all the other Apple devices including the Apple Watch. Developers of applications for the I-Phone and I-Pad often use kits that can contain security leaks such as to the user's identity and potential attack on his or her credit cards according to Appthority and other security reviewers. The same is true for Android applications as well.

IOT Internet of Things

IIOT Industrial Internet of Things

IOE Internet of Everything

IP Internet Protocol. (See also Transmission Control Protocol.)

IPSec An open-standard Internet protocol used for such purposes as establishing secure Virtual Private Network (VPN) communications over public IP-based networks. The packet address header that is stripped off by the IPSec protocol represents a problem for satellite transmission, and thus a special interface protocol must be used for satellite transmissions to avoid such problems with IPSec.
ISD Illicit streaming devices. These are devices, largely available from sources in Asia, that allow illicit access to copyrighted films, programming and other materials.
ISO International Standards Organization, which creates global standards in technical areas including telecommunications and networking. This is also abbreviated OSI, using the French language acronym.
IXP Internet Exchange Points. The modern Internet transitioned over 20 years ago from an entirely governmental network (once known as NSFNET) that was accessed through officially defined network access points (NAPs) to today's network of networks, which includes many private-sector competitors that collaborate to interconnect tens of thousands of networks that are anchored around Internet Exchange Points.
JAVA This is a high level computer language. Java is a general-purpose computer programming language that has the following powerful characteristics in being "concurrent, class-based, and object-oriented." It was specifically designed to have as few implementation dependencies as possible and is intended to let application developers "write once, run anywhere" (WORA). This means that compiled Java code can run on all platforms that support Java without the need for recompilation. Java applications are typically compiled to byte code that can run on any Java virtual machine (JVM) regardless of computer architecture. As of 2016, Java is one of the most popular programming languages in use. The object-oriented aspects of C++ and JAVA allow efficiencies to repeat key functions within a group of processes without repeating all of the steps in the process.
Kernel A kernel is a computer program that is the core of a computer's operating system, with complete control over everything in the system. It is the first program loaded on start-up. It handles the rest of start-up as well as input/output requests from software, translating them into data-processing instructions for the central processing unit. It handles memory and peripherals like keyboards, monitors, printers and speakers. The core function of the kernel is shown in the illustration below.

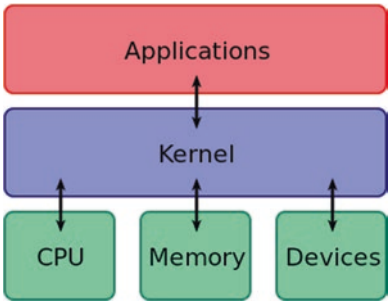

Fig. G.4

Keylogger A keylogger is a type of surveillance software that is typically labeled as spyware. Such spyware has the capability to record every keystroke you make to a log file, usually encrypted. A keylogger recorder can record instant messages, e-mail and any information you type at any time using your keyboard. This is how passwords to electronic financial records at your bank or stockbroker, Social Security records, etc., can be stolen by a "black hat" hacker who is intent on stealing your financial assets.
Kill switch This can be activated to disable a particular web domain.
Knobot This word combines the words "knowledgeable robot." It represents an artificially intelligent robot that is independently able to search the web and carry out other functions independently based on its software algorithms.
LAN Local area network. (Also see MAN and WAN.)
LDAP Lightweight Directory Access Protocol.
Linear economy This is seen as the opposite of a circular economy. Such an economic system tends to be wasteful of resources, does not seek to recycle in production and consumption, and leads to polluting processes. A linear economy is sometimes referred to as being based on a 'take, make, dispose' model of production.
Litecoin This is a form of crypto-currency that is similar in concept and mode of operation to a bitcoin.
Linux Linux has emerged as a popular operating system for web servers such as Apache, as well as for network operations, scientific computing tasks that require huge compute clusters, running databases, desktop/endpoint computing and running mobile devices with Open Systems (OS) versions such as Android. Since its initial development, Linux has adopted the "copyleft" stipulations of the Free Software Foundation, which originated the GNU GPL General Public License (GPL). Copyleft says that anything taken for free and modified must in turn be distributed for free. In practice, if Linux or other GNU components are developed or modified to create a new version of Linux, that new version must be distributed for free. This is the foundation of open source development which prevents a developer or other groups from profiting from the freely available work of others.
Mach Mach is a kernel developed at Carnegie Mellon University to support operating system research and parallel computing. Mach is often mentioned as one of the earliest examples of a microkernel. However, not all versions of Mach are microkernels. Mach's derivatives are the basis of the modern operating system kernels in GNU Hurd and Apple's operating systems macOS, iOS, tvOS and watchOS. Mach 3.0 was the last issue of this software.
Macros A macro is a shortened name for what is called a "macroinstruction" in computer programming. Specifically, in computer science a macroinstruction is a lengthy rule or pattern that specifies how a certain input sequence (often a sequence of characters) should be mapped to a replacement output sequence (which is also typically a sequence of characters). These detailed procedures represent a prime location where malware might be implanted. Enabling the insertion of a new macro is something to be done with caution and only when you have an active antivirus program working on your computer or smart phone.

Malware This term refers to all types of intrusive software that have a malicious intent. Thus included in this concept are such terms as adware, worms, Trojan horses and time bombs, data bombs, viruses, zip bombs, logic bombs, rootkits and bootkits, ransomware, phishing and pharming activities. Thus the generic term of malware refers to all types of software that can be used to carry out some sort of cyber-attack. In terms of volume, there are definite trends in the use of Malware. Trojans now account for nearly 80% all newly discovered malware. This is followed by Adware and/or Spyware that made up almost 14% of the remaining malware. Up to 97% of all new malware can come in the form of Windows Executable files. (Source: Michael Arent, EDS-Global Information Security.)

MAN Metropolitan area network.

Man-in-the-Middle (MitM) This is also sometimes known as Rogue Wi-Fi or sometimes as "Evil Twins." A MitM or Rogue Wi-Fi attack is where a cyber-criminal either sets up a public Wi-Fi hotspot or compromises an existing public Wi-Fi network to attack anyone who accesses it. Sometimes criminals create an Evil Twin hotspot located geographically near a legitimate Wi-Fi provider and then give it a nearly identical name to the trustworthy provider. These various Rogue Wi-Fi networks prey on anyone who tries to use Wi-Fi on their smart phones, laptops, tablets and other Internet-connected devices to access the network, unaware that the criminal has designed it to intercept and/or alter the data that users send and receive. Once connected to such a network, all transmissions become vulnerable to the attacker, who can steal personal information, infect the users' devices with malicious software or even impersonate trusted contacts. Although software can sometimes protect against such attacks by authenticating a secure connection, prudent users should never connect to a Wi-Fi network that is not known and trusted.

Mirai Mirai (Japanese for "the future") is a malware that turns networked devices running Linux into remotely controlled "bots" that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as IP cameras and home routers or smart utilities such as on-line washing machines, refrigerators, etc.

Modbus Modbus is a serial communications protocol originally published by Modicon (now Schneider Electric) in 1979 for use with its programmable logic controllers (PLCs). This protocol, which is simple and robust, has become a de facto standard communication protocol, and it is now a commonly used for connecting industrial electronic devices. The main reasons for the use of a Modbus in the industrial environment is because this protocol was developed: (i) with such industrial applications in mind; (ii) it is openly published and royalty-free; (iii) it is easy to deploy and maintain; and (iv) it moves raw bits or words without placing many restrictions on vendors. Modbus enables communication among many devices connected to the same network, for example a system that measures temperature and humidity and communicates the results to a computer. The concern with Modbus is that it can be attacked by black hat crackers for criminal or terrorist purposes.

MQTT Protocol MQTT (formerly MQ Telemetry Transport) is an ISO standard (ISO/IEC PRF 20922) publish-subscribe-based "lightweight" messaging protocol for use on top of the TCP/IP protocol. It is designed for connections with remote locations where a "small code footprint" is required or the network bandwidth is limited. The publish-subscribe messaging pattern requires a message broker. The broker is responsible for distributing messages to interested clients based on the topic of a message. Andy Stanford-Clark and Arlen Nipper of Cirrus Link Solutions authored the first version of the protocol in 1999.

NBF NetBIOS Frames or NBF protocol is a non-routable network- and transport-level data protocol most commonly used as one of the layers of Microsoft Windows networking in the 1990s. NBF protocol or NetBIOS over IEEE 802.2 LLC is used by a number of network operating systems released in the 1990s, such as LAN Manager, LAN Server, Windows for Workgroups, Windows 95 and Windows NT. Other protocols, such as NBT (NetBIOS over TCP/IP), and NetBIOS-over-IPX/SPX also implement the NetBIOS/NetBEUI services over other protocol suites. The NBF protocol is broadly, but incorrectly, referred to as NetBEUI. This originates from the confusion with NetBIOS Extended User Interface, an extension to the NetBIOS API that was originally developed in conjunction with the NBF protocol; both the protocol and the NetBEUI emulator were originally developed to allow NetBIOS programs to run over IBM's new token ring network. Microsoft caused this confusion by labeling its NBF protocol implementation NetBEUI. NBF is a protocol and the original NetBEUI was a NetBIOS application programming interface extension.

NETCONF The Network Configuration Protocol (NETCONF) is a network management protocol developed and standardized by the IETF. It was developed by the NETCONF working group and published in December 2006 as RFC 4741 and later revised in June 2011 and published as RFC 6241. The NETCONF protocol essentially provides a mechanism that allows network devices to be installed, operated, manipulated and deleted. Its operations are realized on top of a simple remote procedure call (RPC) layer. The NETCONF protocol uses an Extensible Markup Language (XML)-based data encoding for the configuration data as well as the protocol messages.

Network mapper This is a security scanner used to discover network hosts and also identifies services provided. It is also sometime referred to as an Nmap.

Next-Generation Firewall (NGFW) This firewall provides the latest capabilities that are beyond traditional port-based controls and enforces specifically defined policies that are typically based on application, content and/or the user.

NFC Near Field Communications. This is the radio frequency ID (RFID) technology that is being used for instant pay and go systems now being used with credit cards that are registered with credit card banks. There are ongoing concerns about the security of NFC systems and the range at which they work or can intercept information.

NHTSA National Highway Traffic Safety Administration. A U. S. federal agency that addresses vehicular safety in the United States and is involved with creating safety standards for driverless vehicles.

NIST National Institute for Standards and Technology. This is the U. S. agency that is responsible for creating and enforcing standards of all types but especially of weights, measures and technical standards related to communications, power, networking and information. It has been designated as the lead agency for establishing cybersecurity standards and protections for the U. S. federal government. As part of this responsibility it has developed the following standardized process for noting data intrusions and an appropriate response mechanism.

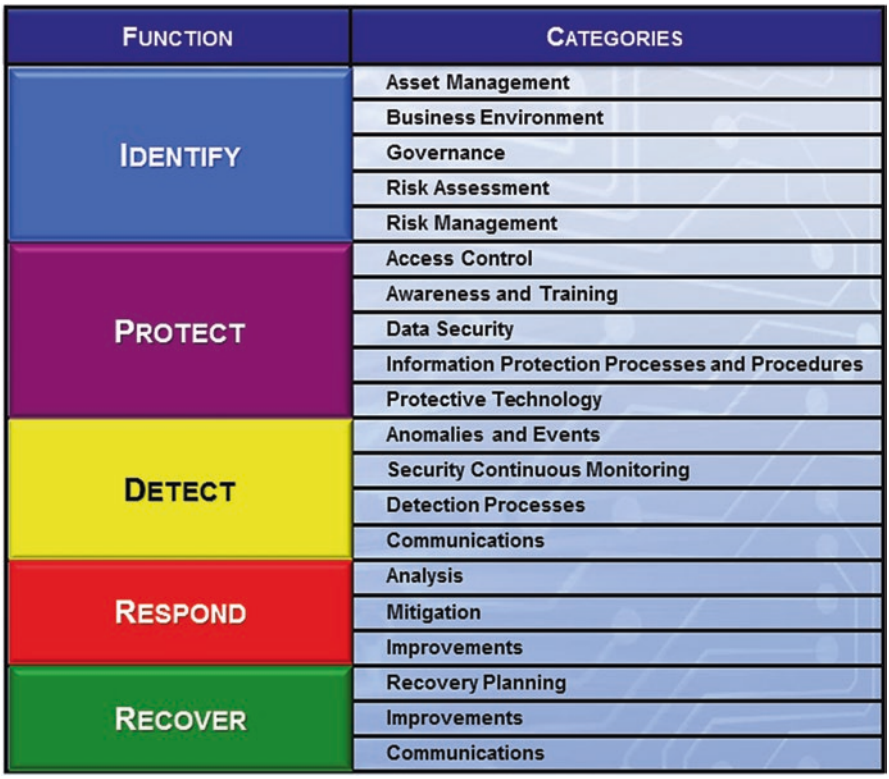

Fig. G.5 The NIST cybersecurity framework for identifying, protecting, detecting, responding to and recovering from data intrusions

NSA National Security Agency.

NTIA National Telecommunications and Information Administration. This is the part of the U. S. Department of Commerce that is responsible for a number of tasks related to assignment and use of radio frequencies with regard to the U. S. federal government's civil governmental functions in contrast to defense or military uses. It also is tasked with furthering telecommunications development and universal access. It is also tasked, along with NIST, in developing data network protective functions for the U. S. government.

OECD The Organization of Economic Cooperation and Development (OECD) that includes many of the world's more economically developed countries such as the United States, Canada, Australia, New Zealand, Europe, and Japan.
OS Operating system.
OSI Open Standards Interconnection model that operates on the basis of seven layers of interconnection that range upward from the physical transmission (level 1) up to the applications layer (level 7). (See table in Chapter 1.)
PaaS Platform as a Service. This relates to companies that utilize the cloud. Platform-as-a-Service (PaaS) solutions from the cloud can now be used both to build and deploy new applications—especially for mobile users. Many PaaS providers have extended their offerings to include so-called back-end infrastructure, namely storage and computing, as needed.
Packet spoofing or IP spoofing The basic protocol for sending data over the Internet network and many other computer networks is the Internet Protocol ("IP"). The header of each IP packet contains, among other things, the numerical source and destination address of the packet. The source address is normally the address that the packet was sent from. By inserting a fake header containing a different address, an attacker can make it appear that the packet was sent by a different machine. The machine that receives spoofed packets will send a response back to the forged source address. This technique is obviously only used when the attacker does not care about the response or has some way of guessing the response. It is sometimes possible for the attacker to see or redirect the response to his or her own machine. The most typical case that packet spoofing might be used is when the attacker is spoofing an address on the same local area network (LAN) or wide area network (WAN).
Persistency attacks The attacker simply keeps on trying again and again until the cracker eventually gets access to the network or a targeted computer.
Petabyte A thousand terabytes, or a thousand trillion bytes of data.
Pharming Pharming is an even more devious way of capturing information than phishing (see below). Phishing attempts to capture personal information by trying to trick users into visiting a fake website. Pharming is an attempt to send users to false websites, but by manipulating the IP website address so that users are not aware that this has happened. Although a typical website uses a domain name for its address, its actual location is determined by its numerical IP address. When a user types a domain name into his or her web browser's address field and hits Enter, the domain name is translated into an IP address. This is accomplished by what is called a DNS server. The web browser then connects to the server at this IP address and loads the web page data. After a user visits a certain website, the DNS entry for that site is often stored on the user's computer in a DNS cache. This way, the computer does not have to keep accessing a DNS server whenever the user visits the website. One way that pharming takes place is via an e-mail virus that "poisons" a user's local DNS cache. It does this by modifying the DNS entries, or host files. For example, instead of having the nine-digit IP address

17.254.3.183 direct to www.apple.com, it may direct to another website determined by the hacker. Pharmers can also poison entire DNS servers, which means any user that uses the affected DNS server will be redirected to the wrong website. (For more information on pharming, go to http://techterms.com/definition/pharming.)

Phishing This is one of the most common categories of online scams. In this case a criminal, often by means of high-volume spam emails and/or the establishment of fake websites set up to appear to be legitimate, convinces victims to provide personal information. This might be such data as private account details, credit card numbers, and/or Social Security numbers. If you receive large amounts of unsolicited email and spam in your inbox, chances are that a fair share of these are not simply online businesses looking for customers but instead devious phishing attempts. Basic phishing attacks do not require a high level of sophistication by the criminal and are therefore easy to perpetrate in high volume. Phishing relies on tricking the victims, and while exercising good judgment and online awareness can generally thwart such attacks, many unwary web users still fall victim to such scams every day. Even if you feel you have a keen eye for identifying scams in your email or are able to avoid visiting harmful websites, cyber-criminals are always working on ways to up their game. It is important to always remain cautious about what websites you visit, how you access them and who you are providing your personal information to online. Remember that the most effective phishing attempts will always appear on the surface to be legitimate commercial communications or links to bona fide websites. Even though an email may appear to be from your credit card company, remember that looks can sometimes be deceiving, and domain names can be tampered with by cyber-criminals. There are different types of phishing activities. (Also see clone phishing, spear phishing, and whale phishing.)

Powerpoint This is proprietary Microsoft software for visual presentations.

Predictive analytics This term can be defined as the practice of extracting information from past recorded performance datasets. This means that relevant historical big data that is available to a city can be used for analytic purposes in processing. These datasets are processed using appropriate algorithms in order to determine patterns and to assist with more accurate predictions of future outcomes and trends based on past performance. Predictive analytics does not pretend to reveal the future, but it provides a good context to determine past patterns of behavior. Such analysis, where correlated with other data, might help reveal why such patterns were manifested in such areas as rates of building of new housing or commercial properties, increases in pollution levels or increased rates of water usage.

Proxy server Proxies were invented to add structure and encapsulation to distributed systems. Today, most proxies are web proxies, facilitating access to content on the world wide web, providing anonymity, and may be used to bypass IP address blocking.

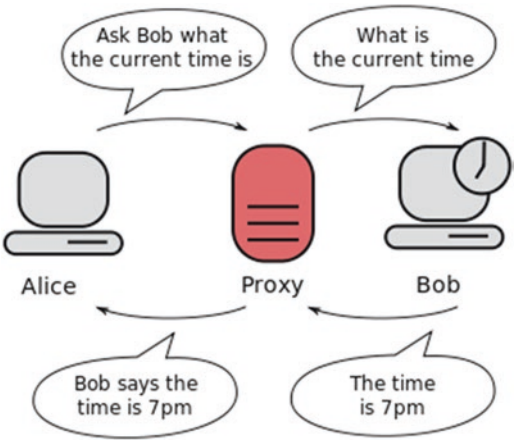

Fig. G.6 Illustration of a proxy server in a computer network accessing the web

Ransomware This is a particular type of Trojan horse that implants malware on a computer so that a special code is needed to unlock a filter that blocks access to all files on a computer. A currently rampant version of a ransomware malware is known as CryptoWall 2.0.

RFC Recommendation for comment. The Internet Engineering Task Force seeks to coordinate recommendations for standardized use of the Internet and its various protocols. This is done by sending out RFCs (recommendations for comment) that are ultimately standardized in terms of usage and technical compatibility within the Internet. Various RFC that are agreed and implemented are assigned numbers such as the User Datagram Protocol (UDP), which is for instance RFC 768.

RFID Radio frequency identification. This simple technology allows for products to be tracked and to be accounted for in inventory. Today an increasing number of credit cards have RFID-enabled capabilities that allow for instant purchase of products by having credit card information read by near field communication readers.

RTSP Real Time Streaming Protocol.

SaaS Software as a Service. This is a term that relates to provision of software to users of the cloud to obtain access to various types of software. See also PaaS (Platform-as-a-Service) and IaaS (Infrastructure as a Service).

SAS Institute SAS Institute (or simply SAS) is an American multinational developer of analytics software whose headquarters are based in Cary, North Carolina. SAS develops and markets a suite of analytics software (also called SAS that derives from the original name, which was Statistical Analysis System). This enterprise, which now nets over $3 billion in revenues and has over 14,000 employees, helps access, manage, analyze and report on data to aid in decision-making. The company is the world's largest privately held software business and its software is used by most of the Fortune 500 companies. Currently SAS and the Electronic Freedom Foundation are in dispute as to how far copyright protection of computer software can extend.

SCADA Supervisory Control and Data Acquisition system that provide the automated 24/7 control and data reporting capabilities for electrical power grids, pipelines, traffic signaling systems, water treatment and distribution, sewerage treatment, and other large networks found within smart cities and national transportation, communications and power systems.

SCP The Secure Copy Protocol (SCP) is a network protocol, based on the BSD RCP protocol, which supports file transfers between hosts on a network.

Seed phrase This is a randomly generated grouping of twelve words generated by MetaMask software that is used to generate 64 random characters that becomes a private key for a blockchain account. This private key is then run through two more transformations to create an address within a blockchain crypto-currency such as bitcoin, Ethereum, etc.

Self-replicating codes These types of programs are able to self-replicate. They are thus able to spread copies of themselves and in the most sophisticated forms are able to distribute modified copies. These can be classified as either virus or worms. These types of malware codes have the ability to propagate and distribute themselves to other users' computers.

Shifting focus of computer attacks on networks In the past decade there have been three notable shifts in the nature and type of computer attacks. These key shifts are: (i) a shift from a desire for notoriety to financial or strategic motives; (ii) a shift from untargeted or indiscriminate attacks to targeted attacks; (iii) a shift from denial of service to stealth components. All types of computer attacks continue to occur, but more and more attacks are focused on illicit financial gain and stealing of computer card, banking or similar data, or on some form of strategic attack on a person, an organization or even a country.

SIM Subscriber Identity Module.

Smart chip for credit cards This is a chip that is inserted into modern credit cards to afford greater protection and to make credit cards much more difficult to counterfeit. These chips are also known as EMV chips. This stands for Europay, Mastercard and Visa, which are the global credit card companies that pioneered the adoption of this type chip. This is now the global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions. In the wake of numerous large-scale data breaches and increasing rates of counterfeit card fraud, U. S. card issuers are migrating to this new technology to protect consumers and reduce the costs of fraud.

Smart city or intelligent community This is a city, town or community that employs computer, telecommunications, sensors and artificial intelligence (AI) systems to upgrade the efficiency and effective operation of its community. These technologies, systems and processes allow the upgraded performance of various infrastructure and key operational units so that the community operations (in real time and for the longer term) not only perform more reliably and at lower cost but are also in a way that is more responsive to the needs of their citizenry while also adjusting to the demographic needs of the community served. This relates not only to infrastructure for energy, transportation, communications, IT systems, water,

sewage, environmental controls, utilities, etc., but also key services such as education, healthcare, police, fire, and EMT. Other urban planners consider this too narrow of a definition of a smart city in placing too much emphasis of ICT technology. These urban planners believe that the concept of "smartness" must also include better mechanisms for citizen involvement in urban planning, balanced zoning, financial incentives, and commercial policies, interdisciplinary and integrated perspectives in planning for the future, and the use of smart data to understand trends and to adapt to changing community needs over time. Finally in light of cybersecurity concerns and techno-terrorist attacks it also means a city that is well-equipped to defend its use of technology and automation against such attacks.

Smart contract This refers to automatically executed pieces of code, typically using a blockchain distributed ledger that can carry value, data or other such condition-based execution. It is most commonly used today for expenditures using bitcoin or other similar crypto-currency.

Smart data This is a concept similar to big data but with greater focus on key interactive variables. This is a type of analysis that is still conducted using large data streams, but in this case the focus is not so much on volume, velocity or variety. Instead the attempt is made to create interactive models of behavior and "systems operations." This focus can help identify the most valuable data to interpret. It can show the results that come from changing the interactions between and among major forces of change. This use of analytics, artificial intelligence, and heuristic algorithms is indeed the key data. The purpose of this type of data analysis is to examine how interactive forces within these proven models reveal patterns of change over time. The object is to develop "actionable" conclusions as to how operations, systems, capital investments, or materials should be altered to provide better and smarter results. The effectiveness of smart data analysis depends on developing the most accurate heuristic tools and interactive models of change within larger systems such as the operational efficiency and growth of a city. Thus the crux of the idea is to identify the most valuable data with the greatest veracity in order to see what is driving change and to see it in a synergistic way.

Smart planning This concept has many aspects. It means using zoning and incentives to concentrate land use intensity around mass transit and to encourage mixed use of residential, commercial retail and office buildings to keep such concentrated areas humming with activity 24 hours a day. It means encouraging good schools, healthcare, parks and recreation, and sustainability of the environmental aspects of a city, including incentives for a circular economy in contrast to a linear economy. Further, it creates opportunity for intensive citizen participation in zoning, longer range civic planning and involvement of citizens and businesses in the city's governance policies. Technological enhancements can be a part of smart planning, but such steps must further the above objectives and advance the city's longer term vision for the future.

Smart traffic signal This is typically a traffic signal system that is also equipped with sensors that can monitor traffic flow and adjust light changes to speed the continuity of traffic throughout a community via networking of these signals together. In some instances traffic signaling systems that are networked together can also

allow a Wi-Fi hot spot to be created on command to respond to the needs of first responders such as at an accident, fire or terrorist attack site.

Source code In computing, source code is any collection of computer instructions, possibly with comments, notations or explanations. These are usually written using a human-readable programming language that can be simple text. The source code of a program is specially designed to facilitate the work of computer programmers. These programmers then indicate in binary code the actions to be performed by a computer. The source code is thus typically transformed by an assembler or compiler into binary machine code understood by the computer. The machine code might then be stored for execution at a later time. The source code, which constitutes a program, is usually held in one or more text files stored on a computer's hard disk; usually these files are carefully arranged into a directory tree, known as a source tree.

Source language Source language and source code are sometimes used interchangeably.

Spy sweepers A spy sweeper is a software product that is designed to detect and subsequently assist in removing spyware and viruses from personal computers. This is not a feature automatically installed in antivirus software and typically involves a premium payment for this service.

Spyware This is software that can monitor keystrokes and other information and allows hackers to obtain personal identification numbers, access codes and other personal information. (See Stalkerware.)

Stalkerware This is a type of spyware that can be loaded onto a cellphone that uses GPS to track where someone goes and can also listen into conversations and record them.

SURTRAC This is a smart traffic signaling and sensor system first developed by Carnegie Mellon University in 2012. The acronym stands for Scalable URbanTRAffic Control.

SYN-Flood Synchronize Flood. This type of DDOS attack creates a flood of ACK (acknowledgement) messages in contrast with SYN floods in which the attacker can use fake, random, non-incriminating source addresses for the packets.

Targeting attacks This type of attack is targeted toward a particular organization's network. It creates an attack website through which many individuals can attack another specific site.

TCAS Traffic collision avoidance system (TCAS), also known as traffic alert and collision avoidance system, is an aircraft system designed to reduce mid-air collisions. It monitors the airspace around an aircraft for other aircraft equipped with a corresponding active transponder and operates independent of air traffic control. This TCAS capability, that ICAO regulations have mandated, be provided on all aircraft over 6700 kg, warns pilots of the presence of other transponder-equipped aircraft and thus reduces the threat of collision.

TCP Transfer Control Protocol.

Terabyte This refers to a trillion bytes of information. The books in the U. S. Library of Congress, the world's largest library, can be calculated in terms of terabytes of information.

Tor Free software that represents a 2nd generation of onion routing. This allows Internet users to communicate anonymously over the Internet.

Tox Tox is a peer-to-peer instant messaging and video calling protocol that offers end-to-end encryption. The stated goal of the project is to provide secure yet accessible links to anyone without any special difficulty.

Translator This is a computer program that translates a program written in a given programming language into an equivalent program in a different computer language, without losing the functional or logical structure of the original computer program. Thus translators can provide translations between high-level and human-readable computer languages such as C++, Java and COBOL, or intermediate-level languages such as Java byte code, or even low-level languages such as assembly language and machine code. There are also translators that can make a translation between software implementations and hardware such as an Application Specific Integrated Chip that utilizes the same programming.

Trojan horse (or simply Trojan) A Trojan horse is a form of computer virus that serves to create a secret or backdoor access to a user's device. (This is a hidden illicit and non-detected entry to a computer.) The hacker, once a Trojan horse is installed, can then have unauthorized access to the affected computer typically to steal data or passwords over a period of time and thus is less likely to be detected since problems will likely occur over time rather than all at once. Trojans horses—or hidden backdoors—are not easily detectable. Computers, however, may appear to run slower. Malicious programs are classified as Trojans horses (or simply Trojans) if they do not attempt to inject themselves into other files (computer virus) or otherwise propagate themselves, which would then be labeled a worm. A computer may host a Trojan via a malicious program. This is usually done by tricking a computer user into executing an installation command. This is often accomplished by opening an e-mail attachment disguised to be unsuspicious. It might be in the form of a survey or access to a coupon or some other download. It might even be disguised as an antivirus program. A Trojan horse that is instructed to be activated at particular time is sometimes called a time bomb.

Troll Someone that deliberately posts derogatory or inflammatory comments to a community forum, chat room, newsgroup and/or a blog in order to bait other users into responding. It is also someone that frequents and eavesdrops on a chat room but does not contribute to it. It can also be an individual or a network of individuals that distributes, under false pretenses or through the use of bots, fake news to influence buying habits or elections.

UAS Unmanned aircraft system.

UMTS The Universal Mobile Telecommunications System (UMTS) is a third-generation mobile cellular system for networks based on the GSM standard. Developed and maintained by the 3GPP (3rd Generation Partnership Project), UMTS is a component of the International Telecommunications Union IMT-2000 standard set. This is being replaced and upgraded to the 4G broadband cellular service, and this in turn will be replaced by an even broader band and more capable 5G mobile service in coming years.

Unix Unix is an operating system that was first developed in the 1960s by AT&T Bell Labs, and has been under constant development ever since, including providing a suite of programs. It is a stable, multi-user, multi-tasking system for servers, desktops and laptops. It was the first such system written in the C, C++ language. Unix has evolved as a kind of large freeware product, with many extensions and new ideas provided in a variety of versions of Unix by different companies, universities and individuals. The original Unix system was discontinued as many people started to make their own operating systems based on Unix. So today Unix is a group of operating systems that all work in the same way based on a "kernel" system. There are differences, but their basic behavior is the same. In the Unix family is Linux, BSD, and Darwin, which is the core of Mac OS X.

Virus A computer virus is loaded without the knowledge of the computer or smart phone user. This malware can display unwanted messages or spam or do something much worse. This might be to corrupt or delete data on your computer, use your email program to spread itself to other computers, or even erase everything on your hard disk. It might be in the form of a time bomb or Trojan horse and thus only reveal itself after weeks or even months have elapsed. Computer viruses are often spread by attachments in email messages or instant messaging messages. There are today a large number of such viruses and worms (see also worms).

VPN Virtual Private Network that was created to allow privacy of transmission over public networks.

WannaCry This is one of the relatively new and pernicious ransomware attack tools that was used in a global cyber-attack that occurred in early May 2017. This attack software is also a worm. This means that once it gets into a computer it looks for other computers to try and spread itself as far and wide as possible.

Web domain The precise identifying address for a particular website.

Website forgery This is a sophisticated type of phishing technique. Website forgery is a malicious attack that creates the illusion of an exact replica of a trusted website on a victim's computer for the purpose of stealing personal information. By taking advantage of vulnerabilities in a victim's computer, a hacker can redirect the user to a forged site that appears completely trustworthy, including the browser displaying the correct URL with a secure connection, but in reality the website is a fake site with a deceptive graphical overlay masking the true URL.

WEP encryption Wired equivalent privacy (WEP) is a security algorithm for the IEEE 802.11 standard for wireless networks. WEP encryption was initially introduced as part of the original 802.11 standard ratified in September 1999, its intention to provide data confidentiality comparable to that of a traditional wired network. WEP, recognizable by the key of 10 or 26 hexadecimal digits, was at one time widely in use and was often the first security choice presented to users. In 2003 the Wi-Fi Alliance formally voted to approve Wi-Fi Protected Access (WPA) as the new standard that should be used to replace WEP. In 2004, the new IEEE standard became 802.11i, which is known as WPA2.

Whale phishing This is another version of spear phishing. It refers to a phishing attack against a senior level individual within a commercial organization, institution or governmental agency. Whalers will target a specific individual with access to

sensitive systems and information. A typical attack would come in the form of an email that appears to be from a customer, business partner, or even a more senior official. The message would likely refer to an urgent business matter in order to trick the victim into clicking on a malicious link or attachment or to reveal key passwords or data. If you work in a high level or key position within your company, you are at an elevated risk of being targeted. Even if you do not consider yourself to be in a senior role, you may still have access to sensitive information within your organization and be targeted as a result. As an agent of your employer, it is important to identify fraudulent emails and take every possible precaution against such attacks.

WiFi Wireless fidelity. This is a wireless local area network that is defined by the IEEE Standard 802.11. Such wireless networks can be publicly available without a password or they can be password protected. To provide a reasonable level of privacy protection these WiFi networks should have a reasonably high level of encryption.

WiFi Protected Access Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, WEP (Wired Equivalent Privacy). A flaw in a feature added to Wi-Fi, called Wi-Fi Protected Setup, allows WPA and WPA2 security to be bypassed and effectively broken in many situations. WPA and WPA2 security implemented without using the Wi-Fi Protected Setup feature are unaffected by the vulnerability.

Windows This is the most commonly used operating system for individual business use and personal computers. This software was developed and marketed worldwide by Microsoft. Windows 10 is the latest version of the personal computer operating system developed and released by Microsoft as part of the Windows NT family of operating systems. It was officially unveiled in September 2014 following a brief demo at Build 2014 and after beta testing had its consumer release on July 29, 2015.

WLAN Wireless local area network. This is a generic name for any wireless data network where a router or Wi Fi system creates a "hotspot" for users to access. The IEEE standard 802.11i is the key specification for a WiFi network.

WORA Write Once and Run Anywhere. This is a feature that is especially applied to JAVA script programming.

Worm A computer worm is a standalone malware computer program. The unique aspect of a worm is that it can self-replicate for the purpose of then spreading to other computers. Often, it uses the Internet to spread itself from the infected computer. Unlike a computer virus, a computer worm does not need to attach itself to an existing program and thus can be implanted anywhere in a computer memory.

WWW The world wide web.

Yoddabyte This is a huge number. It is the equivalent to a trillion terabytes, a thousand zettabytes, a million exabytes, a billion petabytes or a trillion times a trillion bytes of information.

Zettabyte This is a billion trillion bytes of information. It is also equivalent to a 1000 exabytes, a million petabytes, or a billion terabytes.

Zip bomb A zip bomb, also known as a zip of death or decompression bomb, is a malicious archive file designed to crash or render useless the program or system reading it. It is often employed to disable antivirus software, in order to create an opening for more traditional viruses. Rather than hijacking the normal operation of the program, a zip bomb allows the program to work as intended, but the archive is carefully crafted so that unpacking it (e.g., by a virus scanner in order to scan for viruses) requires inordinate amounts of time, disk space or memory. Most modern antivirus programs can detect whether a file is a zip bomb, to avoid unpacking it.

Zombie computers This is a term that is applied to members of large botnets that have been assembled either to launch denial-of-service attacks, to distribute e-mail spam on a very large scale, or to conduct click fraud.

Note: This list of acronyms was developed and is copyrighted by the authors, Joseph N. Pelton and Indu Singh, and is licensed on a one time basis to Springer Press for inclusion in this book.

Index

© Springer International Publishing AG, part of Springer Nature 2019

J. N. Pelton, I. B. Singh, *Smart Cities of Today and Tomorrow*,
https://doi.org/10.1007/978-3-319-95822-4