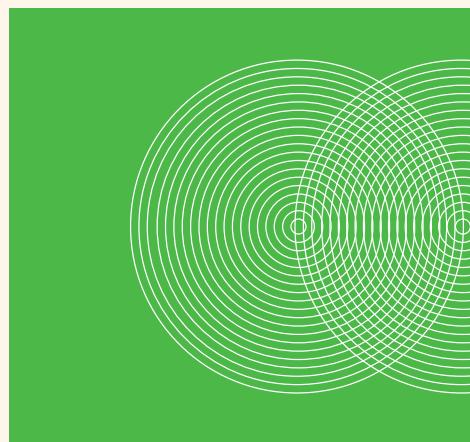
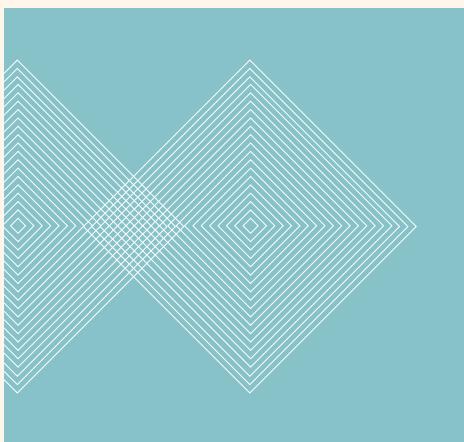
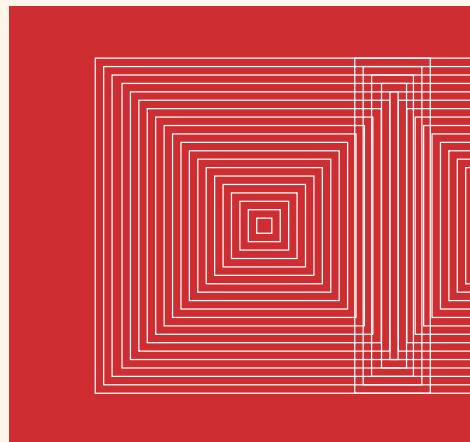
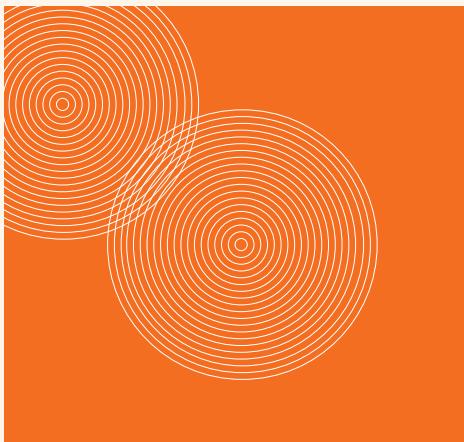


MASSEY DEFENCE AND SECURITY SERIES



Cyber Security and Policy

A Substantive Dialogue

*Edited by Andrew Colarik, Julian Jang-Jaccard
and Anuradha Mathrani*



A world without the advantages and conveniences provided by cyberspace and everything it connects us to is now unimaginable. But do we understand the threats to this massive, interconnected system? And do we really understand how to secure it? Cyber security is no longer just a technology problem; the effort to secure systems and society are now one and the same.

This book discusses cyber security and cyber policy in an effort to improve the use and acceptance of security services. It argues that a substantive dialogue around cyberspace, cyber security and cyber policy is critical, and will enable a better understanding of some of the large security issues we face.

Cyber Security and Policy

A Substantive Dialogue

*Edited by Andrew Colarik,
Julian Jang-Jaccard and
Anuradha Mathrani*



MASSEY UNIVERSITY PRESS



MASSEY
UNIVERSITY
PRESS

Massey Defence and Security Series is an imprint of Massey University Press

First published in 2017 by Massey University Press

Massey University Press, Private Bag 102904, North Shore Mail Centre, Auckland 0745, New Zealand

www.masseypress.ac.nz

Text copyright © individual contributors, 2017

Design by Open Lab. Layout by Kate Barraclough

The moral right of the authors has been asserted

All rights reserved. Except as provided by the Copyright Act 1994, no part of this book may be reproduced, stored in or introduced into a retrieval system or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written permission of both the copyright owner(s) and the publisher.

A catalogue record for this book is available from the National Library of New Zealand

Printed and bound in China by Everbest Ltd.

ISBN: 978-0-9941363-4-3

eISBN: 978-0-9941415-9-0

I have found that it is the small everyday deeds of ordinary folk
that keep the darkness at bay. Small acts of kindness and love.

Mithrandir (J. R. R. Tolkien)

CONTENTS

Foreword	9
<i>Professor Rouben Azizian</i>	
 Introduction	 13
<i>Andrew Colarik</i>	
 Part 1: Cyber Security	
1. Online services authentication	27
<i>Arno Leist and Daniel P. Playne</i>	
2. Emerging cyber-security threats in cloud computing and big data	48
<i>Julian Jang-Jaccard</i>	
3. Revenue fraud in e-commerce platforms: Challenges and solutions for affiliate marketing	67
<i>Bede Amarasekara and Anuradha Mathrani</i>	
4. Picking high-level fruit in dark trees: Using complex systems analytics to detect and understand crime	87
<i>David Robinson and Chris Scogings</i>	
5. Cyber counterintelligence: Concept, actors and implications for security	109
<i>Courteneay J. O'Connor</i>	

Part 2: Cyber Policy

6. Challenges in governance of cyber neutrality <i>Thomas Potter</i>	131
7. The internet of things: Cyber-security challenges and policy solutions <i>Des T. R. Gilmore</i>	144
8. Limitations of cryptography within the information security environment <i>Robin Behersing</i>	161
9. The failure of public and private sector regulation in cyber security: A Singaporean case study <i>Paul A. Watters, Jacqueline Ziegler, Seung Jun Lee & Maya F. Watters</i>	177
10. Globalisation and the rise of the jihadist virtual network <i>Nicola Port</i>	203
11. Snowden and GCSB: Illuminating neoliberal governmentality? <i>Damien Rogers</i>	217
About the editors	240
About the contributors	242

FOREWORD

This publication on cyber security and policy represents a comprehensive and interdisciplinary security analysis that has a broad academic and practical relevance. It demonstrates the increasing complexity, unpredictability and vulnerability of the global and national security environments through the prism of cyber activity. The authors offer well-researched and at times passionate perspectives on evolving cyber trends, government reactions and cyber policies, societal dilemmas with technology, criminal and extremist exploitation of the cyber space, and the vulnerabilities of the cyber infrastructure.

Rapid progress in technology and the unstoppable force of globalisation — occasional isolationist bravado notwithstanding — pose challenges to governments and societies, law and order, and established security paradigms, rules and behaviours. The world of cyber security is in flux. Current and emerging technologies are allowing threats and capabilities to

change the way cyber defences are designed, implemented and presented to customers. It is critical that cyber-security experts and leaders around the world understand the complex trends and underlying dynamics shaping the future of their sector. The loud cyber alarm bells are a powerful reminder that a proper response — not to mention a more desirable but harder to achieve preparedness for emerging security challenges, such as cyber, that are often immune to traditional tools of mitigation — requires a new way of thinking and acting in the national and international security domains.

New Zealand's Cyber Security Strategy 2015 was a clear reflection of the scale and complexity of the problem. Its four goals — cyber resilience, cyber capability, addressing cybercrime and international cooperation — resonate with governmental, business and individual cyber concerns. Almost one million New Zealanders are affected by cybercrime each year, and a recent report put the cost of cybercrime to New Zealand at \$257 million in 2015.

In the past, New Zealand's geographic location has helped keep the country safe from traditional forms of attack. It does not, however, protect the nation from cyber terrorism or cybercrime. The implementation of the strategy is a much more challenging task, as was evidenced by the heavy attendance at the New Zealand Cyber Summit on 5 May 2016, where many speakers and participants stressed the need for more expert advice, government support and collaboration.

Getting businesses to cooperate on cyber security seems almost as hard as prompting rival nations to join efforts against cyber terrorism and cybercrime. Self-interest and the desire to gain a competitive edge in the cyber domain still obstruct reasonable pragmatism and common security. Clearly, old habits will need to change.

This very helpful volume offers a different way of approaching cyber issues. It is written by both established and emerging scholars, and is a good example of a much-needed collaboration on cyber issues that crosses not just disciplines but also academic research and experience. Fresh and

innovative perspectives are as important as mature scholarly opinion. It combines broad strategic and political issues with specific technical facts, and brings together experts from a wide variety of academic disciplines. It is a reminder that the security train has left the old station, owned and operated by uniformed forces: the ‘battle’ for cyber security is too important to be left to traditional security agencies.

*Professor Rouben Azizian
Director, Centre for Defence and Security Studies
Massey University*

INTRODUCTION

*Andrew Colarik
Centre for Defence and Security Studies
Massey University*

The realm of digital communications has fostered unforeseen changes in the expansion of the economy, societal connectivity and even broad political change. A 2011 report issued by McKinsey Global Institute stated that over two billion people are connected to the internet and an additional 200 million are added each year. Of the 13 countries studied, the internet comprised 3.4 percent of gross domestic product (GDP), and 21 percent of GDP growth in the last five years (McKinsey Global Institute, 2011). With a reported 1.72 billion Facebook users worldwide sharing huge amounts of personal and professional information, the ability to connect with people anywhere around the globe is staggering (Statista, 2016). This in turn has led to social media impacting the way news is communicated and, in fact, affecting the stability of repressive regimes. No one could have foreseen that the arrest and torture of Kareem Al-Beheiri would be the trigger point to launch the Arab Spring through a cyberactivism network throughout the Middle East and the rest of the world (Khondker, 2011). All these activities and much more have been facilitated by cyberspace to a degree

where individuals, organisations and nations are wholly dependent on its persistent and reliable operation. Throughout this book, the authors will explore this problem space and offer a variety of perspectives, discussions and solutions on some of the current issues happening in cyberspace.

WHAT IS CYBERSPACE?

Ever since the invention of the telegraph in 1827, the range and reach of communications has brought people closer together, integrated processes and daily activities, and increased the speed with which people can act on both good and bad information. What started as a single wired medium evolved to cross oceans, switched a multitude of commercial lines and migrated into the wireless mediums that make global communications possible. Next came the birth of the Advanced Research Projects Agency Network (ARPANET) in 1969. This was followed by the invention of the Transmission Control Protocol (TCP) in 1974 and the World Wide Web in 1992, both of which are the foundations of the internet of today.

From there came all the various products and services that have led to smartphones with significantly more computing power than was used to put man on the moon; applications that facilitate everything from electronic wallets to measuring your heart rate and alerting emergency response units; and a connectivity on the scale never before seen in human history. Welcome to cyberspace; the on-demand place for all your computing and connection needs.

From a purely academic perspective, the term 'cyber' is a made-up word for something that is composed of a collection of digital technologies. It includes the physical infrastructures and telecommunication devices that allow for the connection of communication system networks such as servers, computers, tablets, smartphones and other devices. Supervisory Control and Data Acquisition (SCADA) systems that support critical infrastructure such as power and water distribution are also included in this basket of technologies. Essentially, most computer systems, their related software, the networks that connect them and the data that flows

through them are what we refer to as cyberspace. The progression from a series of digital taps transmitted over a wired medium has transformed people's daily activities with 'what is commonly understood as modern conveniences'.

The technologists of the world, through loose collaboration and building on each other's innovations, have created what George Whitesides calls 'stacked simplicity'. By starting at the simplest levels of system design and building additional layers of usability, the internet has become in relative terms 'reliable, predictable, repeatable' (Whitesides, 2010). It is these very characteristics that have allowed for its widespread acceptance and proliferation. However, this has also been the foundation for why the internet is being exploited by those who put self-interest before all others, and this in turn is driving the need to provide cyber security.

There is a growing understanding that network and information security is an important prerequisite for economic growth and national security (Tauwhare, 2016). Banking and finance are now nearly all digital processes, and trading exchanges are globally connected. Transportation systems, logistics and supply chains would halt without the coordination that digital systems provide. Power plants — both hydroelectric and nuclear — and the electrical grids that distribute power provide this all-important commodity through a series of communication pathways that keep capacities balanced and people's dwellings lit, warm and convenient. Medical histories, diagnostic devices, emergency response and care are extremely hampered when access to these supporting systems is absent. And, as previously discussed, the relationship between citizens and their governments relies on the effective and dependable communication these technologies provide.

It is precisely at this point that benefit turns into consequence: we value the advantages and conveniences that cyberspace brings to society. But are we really prepared for what must be done to secure this massive, interconnected system?

WHAT IS CYBER SECURITY?

The founding pillar of all security is trust, and cyberspace is no different. The level of trust earned or blindly accepted determines the longevity of the trust relationship. While mechanical devices have a high degree of reliability — and the internet can be viewed as an expansive set of mechanisms — their application towards building a trustworthy environment is ultimately determined by the people who design, build and use these systems. Therefore, cyberspace first and foremost relies heavily on people to provide its security.

Currently, those tasked with securing cyberspace are made up of a basket of design, organisational and technical specialisations, including network security, information security, infrastructure protection and other support processes whose primary roles are to mitigate the inherent risks of this environment. What this means is that there are many different technologies, configurations and arrangements of technologies, organisational uses and a wide variety of institutional priorities to contend with when dealing with cyber security. In most cases these are complementary; in others they are competing.

Cyberspace is an evolution from a diverse set of technologies that have been layered on each other, and the truth is that no one party has total control over the rules set for its use. The so-called standards that govern the internet are published by the Internet Engineering Task Force (IETF), but even these are simply industry guidelines. The actual implementations are governed by the organisations that are funding the efforts. The system is an organic structure in a technological sense. The same can be said for everything and everyone plugging into cyberspace: all have different agendas and leverage the technology for their own gains. So let us first look at the services these professionals provide and, in turn, what many of us demand of security in cyberspace. What are these services and how do they align with the demands of security in the ever-growing cyberspace?

There are three primary services, and four more derived from these, that comprise what is commonly understood as cyber security. The first three

are confidentiality, integrity and availability. Often referred to as CIA, these are the foundations from early in the establishment of digital information-security best practices. The SANS Institute Glossary of Security Terms (SANS Institute, 2016) defines these as:

- Confidentiality — the need to ensure that information is disclosed only to those who are authorised to view it;
- Integrity — the need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete; and
- Availability — the need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it.

Beyond these three, security services can be further expanded to include:

- Access control — provides protection of system resources against unauthorised access through access control lists and ticket-granting mechanisms;
- Non-repudiation — the ability for a system to prove that a specific user and only that specific user sent a message and that it hasn't been modified;
- Auditing — the information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities (SANS Institute, 2016); and
- Accountability — the defining and enforcement of the responsibilities of the participating parties.

While it is recognised that there are other services that are not included in this list, it is these seven that comprise the bulk of security activity in this space. When we consider the efforts to secure cyberspace, it comes down to how practitioners leverage their individual expertise towards achieving these services. Some of this is in the form of technologies such as encryption in the case of confidentiality, integrity and non-repudiation; resiliency and redundancy in the case of availability; identity verification mechanisms for access control; and audit trails (auditing) and vulnerability

testing for accountability; however, it also encompasses organisational standards, processes and policy. But cyber security does not just stop there; or, rather, there are aspects of cyber security that involve efforts to leverage these services and other mechanisms in order to improve the people component of this immense effort. It is this very combination that is represented throughout this volume.

The first section of this book (chapters 1 to 5) discusses cyber security in an effort to improve the overall security for systems and the people using them. A few of the chapters are technical in nature, but they will illuminate some of the more foundational concepts that link the basic security mechanisms we rely on.

In chapter 1, ‘Online services authentication’, the authors provide an overview and discussion of modern authentication techniques and protocols, including OAuth, OpenID Connect, SQRL (Secure, Quick, Reliable Login) and UAF (Universal Authentication Framework), and the use of multi-factor authentication (MFA). These are presented to show the trend away from standard username and password-based authentication methods. This chapter will provide the reader with a solid understanding of the current state of authentication.

In chapter 2, ‘Emerging cyber-security threats in cloud computing and big data’, the author gives an overview of the emerging threats and vulnerabilities in cloud and big data infrastructures. This is followed by a critique of existing state-of-the-art mitigation techniques, and why they do or do not work. The author also offers speculative observations on the direction of future research.

In chapter 3, ‘Revenue fraud in e-commerce platforms: Challenges and solutions for affiliate marketing’, the authors present a case study of an online car-rental company that has subscribed to an affiliate marketing (AM) network. This study was conducted to understand the possible revenue fraud scenarios derived from the ‘cookie stuffing’ exploit in e-commerce platforms. They then offer technical solutions that are effective in recognising this type of fraud activity.

In chapter 4, ‘Picking high-level fruit in dark trees: Using complex systems analytics to detect and understand crime’, the authors examine the application of a more holistic view of crime in the context of the entire criminal problem space or system. This effort is offered to enable criminal events and criminal actors to be detected throughout the entire fabric of criminality. The authors argue that, by leveraging digital technology and the analytics afforded it, patterns can be deduced that will lead to targeting the primary culprits who are perpetrating criminal activities.

In chapter 5, ‘Cyber counterintelligence: Concept, actors and implications for security’, the author examines the use and exploitation of the cyber domain by practitioners of intelligence and counterintelligence, and presents an examination of the intelligence collection methods in cyberspace. She then discusses the implications in the use of cyber counterintelligence, and considers future avenues of research in the field. This chapter provides an excellent transition to the second section of the book, focused on cyber policy, as it illustrates the need for a larger discussion on the direction and governance of cyberspace and its uses.

WHAT IS CYBER POLICY?

There is a growing understanding within organisations that cyber security is no longer just a technology problem: breaches can cause reputational damage, unfair competitive advantage and loss of innovation and intellectual property (Scully, 2014). As a result, promoting initiatives such as cyber resiliency, reduced cybercrime and the development of capabilities and policies in cyber defence is now rising to new levels of national priority (Tauwhare, 2016). The threat that cyberspace presents encompasses the security imperatives of border defence; military security; security of society and environment; security of governance; and the blended national, transnational, international and global security space (Choucri, Madnick & Ferwerda, 2014). It is precisely the need for this important discussion on policy that the second section of this book is designed to address.

Traditionally, what people have deemed to be policy regarding information and communications technology (ICT) has rested at the organisational level of governance. This means there are a multitude of standards and best practice for individual organisations using ICT in order to mitigate its inherent risks to their stakeholders. These provide an impact at the tactical and operational levels of an organisation and often come in the form of a very large book that enumerates levels of responsibility and sets of procedures governing the activities and responses to problems that arise within that particular environment. Several of the chapters in the first section of this book contribute to this effort and present the prevailing wisdom in current research.

However, what is also needed is a strategic level of thinking that transcends individual organisations and instead spans industry sectors and whole-of-society security efforts. People have been content to leave technical issues to the so-called geeks to resolve, and bureaucratic procedures to enforce their conformity, but these organisational-centric approaches have inherent limitations in terms of a holistic cyber-security effort. This is where cyber policy provides value and forms the basis for strategic-level thinking.

The Merriam-Webster Dictionary defines policy as ‘prudence or wisdom in the management of affairs’ with the intention ‘to guide and determine present and future decisions’ (Merriam-Webster, 2014). For purposes of cyber security, policy can be viewed as a macro-level perspective with the goal of informing an audience of a persistent or emerging cyber-security issue, examining that issue in depth and offering pathways for its mitigation and/or resolution. In some cases the target audience may be the general populace, in order to raise awareness of the matter for dialogue and discourse; in others it may be with the objective of mobilising and influencing collective action on the matter. While I acknowledge that this concept of cyber policy is relatively new, some point of origin needs to be established for its context, on the understanding that future authors will further define and clarify the term. In fact, this definition is offered

in the spirit that there needs to be ‘something’ that sits in between private practice and government law or regulation (Carr, 2016). Cyber policy does just that by providing the needed analysis and discussion for professional practice to consider how best to manage the issue, while opening the door to government intervention if the issue cannot be resolved to societal standards.

The second section of this book, chapters 6 to 11, discusses cyber policy in an effort to improve the use and acceptance of security services. It also considers the deployment mechanisms that have an impact on society’s overall security. Lastly, it puts into context the importance of managing the governance of cyberspace.

In chapter 6, ‘Challenges in governance of cyber neutrality’, the author examines the responsibilities owed by internet services that are provided in times of war. This chapter investigates the concept of neutrality and how it is applied in cyberspace. It then discusses potential approaches to resolving the lack of treaties in this space.

In chapter 7, ‘The internet of things: Cyber-security challenges and policy solutions’, the author provides detailed insight into smart devices and the increased connectivity they represent. The chapter enumerates some of the larger security issues associated with these devices and the lack of policy governing this emerging technology. Finally, it presents a policy framework that addresses some of the prevailing issues associated with these technologies.

In chapter 8, ‘Limitations of cryptography within the information security environment’, the author examines the role that cryptography has played in providing information security and, more importantly, the notion of security that cryptography instils. The chapter goes on to discuss the larger role and impact that this perception has on creating an insecure environment. Finally, the author suggests greater cooperation between national cyber-security agencies and the public/corporate spheres as a stronger pathway for best practices to be implemented.

In chapter 9, ‘The failure of public and private sector regulation in cyber

security: A Singaporean case study', the authors suggest that because of the distributed and decentralised nature of internet governance, traditional governments have largely failed to mount effective responses against content that is illegal within their jurisdiction. The case study in this chapter details an analysis of cloud-based advertising in 5000 webpages downloaded in Singapore from rogue websites. The chapter then presents a discussion of the limitations of cyber policy in a neoliberal regulatory environment.

In chapter 10, 'Globalisation and the rise of the jihadist virtual network', the author gives an overview of the use of cyberspace by jihadist groups that are increasingly operating as virtual organisations, recruiting members online and teaching them how to carry out acts of jihad from their current location rather than making physical contact with other members of the organisation. The chapter discusses the fundamental issues that have led to the creation of these virtual organisations, and investigates the factors that have allowed these groups to recruit members successfully. The author then gives recommendations developed with an awareness of the fundamental elements that have given rise to these issues.

In chapter 11, 'Snowden and GCSB: Illuminating neoliberal governmentality?', the author offers a brief insight into the capacity of Edward Snowden's unauthorised disclosures to cast light on the New Zealand Government Communications Security Bureau (GCSB)'s operational activities, strategic partnerships and organisational purposes. The chapter discusses the gaps between what is officially acknowledged and what remains secret, and raises important questions about the use of New Zealand's surveillance apparatus. The author suggests that the response to Snowden's revelations is nothing short of a radical transformation of the state's capability to monitor and control the population of New Zealand.

FINAL THOUGHTS

As the world continues to invest in increasing the range and reach of communications and integrating our futures into the digital realm, it is

our hope that through continued discussions such as those presented in this book we secure this space for our mutual benefit. This book brings together the work of researchers, academics, students and practitioners who, in their own way, demonstrate that the effort to secure systems and society are now one and the same. It presents the positive perspective that a substantive dialogue around cyberspace, cyber security and cyber policy can occur in such a manner that everyone walks away with a better understanding of some of the larger security issues we are facing today.

REFERENCES

- Carr, M. (2016). Public–private partnerships in national cyber security strategies. *International Affairs*, 92(1), 43–62.
- Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for cyber security: International responses and global imperatives. *Information Technology for Development*, 20(2), 96–121.
- Khondker, H. H. (2011). Role of the New Media in the Arab Spring. *Globalizations*, 8(5).
- McKinsey Global Institute (2011). Internet matters: The Net's sweeping impact on growth, jobs and prosperity. Retrieved from http://www.mckinsey.com/~media/McKinsey/Industries/High%20Tech/Our%20Insights/Internet%20matters/MGI_internet_matters_full_report.ashx.
- Merriam-Webster (2014). *Merriam-Webster's Collegiate Dictionary* (11th ed.). Springfield, Massachusetts: Merriam-Webster.
- SANS Institute (2016). Glossary of security terms. Retrieved from <https://www.sans.org/security-resources/glossary-of-terms/>.
- Scully, T. (2014). The cyber security threat stops in the boardroom. *Journal of Business Continuity & Emergency Planning*, 7(2), 138–48.
- Statista (2016). Number of monthly active Facebook users worldwide as of 2nd quarter 2016. Retrieved from <http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>.
- Tauwhare, R. (2016). Improving cyber security in the European Union: The network and information security directive. *Journal of International Law* (June).

Whitesides, G. (2010). Toward a science of simplicity. Ted Talks. Retrieved from https://www.ted.com/talks/george_whitesides_toward_a_science_of_simplicity/transcript?language=en.