INFORMATION SYSTEMS, WEB AND PERVASIVE COMPUTING SERIES

COMPUTING AND CONNECTED SOCIETY SET

Volume 2

Darknet

Geopolitics and Uses

Laurent Gayard

iSTE

WILEY

Darknet

Computing and Connected Society Set

coordinated by
Dominique Carré and Geneviève Vidal

Volume 2

Darknet

Geopolitics and Uses

Laurent Gayard

iSTE

WILEY

First published 2018 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

Library of Congress Control Number: 2018932685

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN 978-1-78630-202-1

Contents

Preface

"According to Stanford[1], by 2030, we will have 130 billion objects connected to the Internet. Even our hands and our hearts no doubt, everything will be connected. What is the governance framework? What public policy will regulate this?"[2] Fadi Chehadé, director of ICANN's 55th Congress, summed up some of the issues raised in this book, by asking these questions during the "high-level government meeting" of several government officials. The statement from the president of the powerful *Internet Corporation for Assigned Names and Numbers* recalls the importance of the ongoing global negotiations between governments, intergovernmental organizations and international institutions on the issue of Internet governance. Since its inception in 1998, ICANN has assumed the essential and strategic role of managing domain names and electronic addressing on the Internet and is a private law organization. However, it is subject to the courts and the U. S. Chamber of Commerce and is therefore dependent on the U.S. government. In 2014, the United States agreed to initiate a transition process paving the way for the internationalization of ICANN and thus, in part, Internet governance. Internationalization or privatization? The future of the Internet depends on resolving this issue,

[1] Stanford University. Private American University, located in the heart of Silicon Valley, south of San Francisco. In 1968, Stanford University was linked to the University of Los Angeles (UCLA) and the University of Utah through the first offshore computer network that took the name ARPANET and foreshadowed the creation of the Internet.

[2] Fadi Chehadé, Director of the *Internet Corporation for Assigned Names and Numbers* (ICANN). 55th ICANN Congress, Marrakech, March 7, 2016.

which remains a source of conflict in the current state of negotiations. These discussions between States, private stakeholders, user communities and international organizations, about the evolution of international jurisdiction that frames the development of the global network, reveal how Internet governance is a major geopolitical issue. While these negotiations were taking place at the highest level, the scale of cyber-attacks that hit hundreds of countries and institutions around the world in May and June 2017, and an even higher number in private institutions, suddenly brought a new type of conflict and criminal activity to the front lines, using cyberspace as its setting. Parallel to the debate on the future status of ICANN, the *Darknet* phenomenon, which encompasses all encrypted, private and alternative networks on the Internet, alternatively raises the issue of network governance and control through the prism of cybersecurity and the preservation of anonymity and freedom of Internet users, another debate, no less essential, which has become even more acute since Edward Snowden's revelations. Because darknets – it is more accurate to speak of "hidden networks" in the plural – participate in an anarchic development of the global network, which is largely beyond the control of states and ICANN, and also because the tools of future wars and computer attacks are exchanged at the heart of these new virtual territories, this book will be devoted to the history and geopolitics of the darknet. Therefore, it will be necessary to start by defining the terms used, starting with darknet and darknets, a plural term to designate various private or encrypted networks, such as Tor (*The Onion Router*), I2P or Freenet, and a singular term to encompass the whole phenomenon of the "hidden Internet". The shift from plural to singular in itself sums up some 15 years of evolution and the transition from the first peer-to-peer (P2P) to the genuine nebula of parallel networks, an evolution that will be discussed at length in this book. An attempt will therefore be made here to differentiate the different spaces that constitute the "network of networks" today ("surface web", "deep web" and "hidden networks"), to explain some essential notions such as network neutrality and to highlight the role of Internet governance operators, such as ICANN. We will then discuss the genealogy of the phenomenon of darknets, which has been placed in the history of the Internet and the transformations of cyberspace. We will try to analyze which cultures are linked to the constitution of the communities and spaces that make up these new virtual territories and lastly, the security, geopolitical and economic implications of this new (r)evolution of the digital universe that we have taken the liberty of calling “Internet 3.0”[3]. We hope that this book will at least partially enlighten the reader on the essential issues of the transformation of the communication society that could change digital usage, public policy and, of course, our daily life in the near future.

Laurent GAYARD

February 2018

[3] By clearly distinguishing this expression from “Web 3.0” that implies the “Internet of Things”.

Introduction

On October 17, 2011, the Anonymous group launched a “darknet operation”, revealing the existence of some forty pedophile sites hosted on the Tor network[1]. The accounts of 1,626 users of these sites were put online and the operation led to the closure of the targeted sites, but the authorities were concerned about the ability of groups such as Anonymous to seriously interfere with ongoing police operations in this type of case. The case also helped to accredit and popularize the idea that there would be a “deep Internet”, providing safe haven for activities under the guise of a vast virtual lawless zone. A year and a half later in August 2013, the FBI’s dismantling of a vast network of child pornography on the Tor network, followed by the arrest of Ross Ulbricht in October of the same year, accused of administering Silk Road, an online drug dealing site, helped fuel the dark legend. The darknet has therefore crossed the threshold of confidentiality and moved from a rumor to a social phenomenon, to the point of capturing French Interior Minister Bernard Cazeneuve’s attention, who in March 2016, did not hesitate to assert in a political context, marked by a wave of murderous attacks and a state of emergency: “Those who hit us use the darknet and encrypted messaging”, he said. A phenomenon known very little of until then, the existence of hidden networks such as Tor, the “onion router”[2], reached a little media fame at the time.

[1] http://www.humanite.fr/medias/un-reseau-de-plus-de-1500-%C2%AB-pedophiles-%C2%BB-demantele-par-anonymous-482267.

[2] Attributing to sites and users connected to the Tor network addresses in “.onion” instead of the classic “.com” or “.fr”.

In 2016, Sir David Omand, former director of GCHQ[3], noted in the pages of the *World Policy Journal* [OMA 16] that: “The so-called darknet is where most of the online criminal activity takes place, largely beyond the reach of law enforcement. On the darknet, anonymity is the rule, and the identity and location of the participants can be concealed from even the most persistent gaze of police and intelligence agencies”. While using the singular term, David Omand nevertheless took care to restore the term darknet to its multiple singularity, which refers to a disparate aggregate of virtual places, since there are actually as many darknets as there are encrypted and private networks. “The darknet is a collection of networks and technologies used to share digital content”, explained Peter Biddle, Paul England, Marcus Peinado and Bryan Willman in 2003, typically considered to be the first individuals to use the term in an article published in 2003. The darknet is not a physically separate network, but applications and a layer of protocols superimposed on existing networks. The four authors included P2P networks, key-protected exchange systems and even electronic messaging, private forums and newsgroups[4] in the denomination of darknets, the term already pluralized. As early as 2003, the four researchers predicted the irremediable expansion of this phenomenon [BID 03]: “We expect that the effectiveness of the darknet as a distribution mechanism will run into some obstacles in the short term, but ultimately, the genius of the darknet will be indelible”.

In 2003, Biddle, England, Peinado and Willman combined the idea of the darknet exclusively with illegal distribution networks for licensed content. The problem that arose at that time, synthesized in the study of the four engineers, was still limited to illegal downloading and the threat posed by this growing phenomenon to the cultural industry. But if the origin of the darknet concept can be linked to the development of illegal download networks, the term also refers to a specific culture linked to technological developments marking the turn of the 20th and 21st century. On February 8, 1996, U.S. President Bill Clinton signed the Telecommunications Act, accompanied by the Communications Decency Act. This initiative

[3] *Government Communications Headquarters* (GCHQ).

[4] *The Network News Transfer Protocol* (NNTP) is a network protocol designated by URLs beginning with news: //. For example, the Usenet network system, invented in 1979, is organized around the principle of newsgroups, which are hierarchical according to different themes, to which a user can subscribe according to their preferences. Newsgroups allow the exchange of articles and even image, audio or video files in some cases.

represented a historic step in the process of liberalizing telecommunications and online services such as the Internet. The Telecommunications Act replaced the old Communications Act of 1934, attempting to take into account the radical changes in American society during the 1960s, 1970s and 1980s. The main idea of the legislation was to foster the development of competition in the telecommunications sector and to facilitate the entry of large private groups into a sector originally dominated by the American Telephone & Telegraph Corporation. Initially intended to promote the opening up of the telecommunications market to multiple groups, the Telecommunications Act actually led to the creation of new telecommunication giants and the disappearance of a large number of minor operators in this sector. Many observers accused the Telecommunications Act of having paved the way for the complete domination of the mass media. In this case, the new legislation allowed a few major operators to take over the market of internet access providers, such as UUNet (now Verizon), Sprint Corporation, Level 3 Communication (acquired on October 31, 2016 by Centurylink), Comcast and AT&T. In the aftermath of Bill Clinton's announcement that he had signed the Telecommunications Act, John Perry Barlow, co-founder of the Electronic Frontier Foundation[5], drafted a "Declaration of Independence of Cyberspace"[6], in which he stated that no government, corporation or institution should impose its authority or claim on any property rights over the Internet. In particular, the declaration, which was addressed to governments and leaders of major economic consortia, proclaimed: "You are not welcome here. You have no sovereignty where we meet. We form our own social contract". The "cyber-revolutionary" rhetoric, such as that of John Perry Barlow, may seem quite fanciful today. However, it still applies today, through multiple small groups, individual operators, sites and discussion forums, fervently defending the idea of a "Freenet" instead of a darknet, in order to reintroduce the name given to the social network created in 2010: an anonymous and free Internet 3.0, on which the user always remains "in control".

However, 20 years after the publication of the "Declaration of Independence of Cyberspace", times have changed, as has the Internet.

[5] Founded in 1990 in the United States by Mitch Kapor, John Gilmore and John Perry Barlow, the Electronic Frontier Foundation's main objective is to defend freedom of expression on the Internet.

[6] See the text in Appendix 1.

According to figures from the Data Observatory[7], the global volume of online databases has reached 4.4 zettabytes[8]. The International Data Center[9] predicts that this global volume will increase 10-fold by 2020 to 44 zettabytes[10]. The exponential rate of development of the Internet today makes any calculation partially obsolete: some authors state a trillion pages have been created, that is to say a thousand billion, etc. [PIS 08, p. 188]. This exponential growth interests public and private companies, anxious to take advantage of the economic opportunities offered by the "deep web" and "Big Data". It also opens up new opportunities for all those who intend to benefit from the growth of the global network, which increasingly calls into question the ability of state structures to effectively monitor the multiple networks that make up the Internet today. This desire to escape the control of institutions responds to economic and ideological motivations and is in line with the promises, sometimes illusory, of a globalized system that makes all forms of borders, barriers and regulations obsolete.

The recent development of darknets, which are no longer just networks of exchange, but real layers of alternative networks superimposed on the global network, contains all the questions raised by the exponential growth of intangible flows, the modification of digital usage and the questioning of the regulatory status of States. The latter, as well as the security and intelligence agencies that depend on them, are now becoming aware of the danger attached to the idea of virtual lawless zones that are somewhat or totally beyond their control. All of them are therefore stepping up their efforts to develop credible and effective policies in the field of cybersecurity. The resurgence of terrorism, but also other illegal activities such as trafficking in

[7] Data Observatory, July 2014, IDC study for EMC-Digital Universe.

[8] 1 zettabyte = 1,000 exabytes, that is to say 1,021 bytes, the basic unit measuring the volumes of digital information. By way of comparison, 1 zettabyte corresponds to 152 million years of viewing standard VHS cassettes.

[9] In 1976, a group of scientists founded the GSE (Group of Scientific Experts) in Geneva at the end of the Geneva Conference on Disarmament in order to study technological developments. Between 1984 and 1995, a series of experiments on improving data collection were carried out jointly by American, Russian and Swedish scientists. In 1996, after the creation of the Comprehensive Nuclear-Test-Ban Organization (CBTO), the International Data Center was transferred from Arlington, Virginia, to Vienna, Austria, to officially become the IDC. Since then, this international organization has generated independent studies and data analysis in a wide range of fields.

[10] According to linguist Mark Liberman, this is the equivalent of all the words and languages spoken on the planet.

drugs, weapons and human beings, which are using new technologies in order to develop, is giving rise to policies for the security and surveillance of cyberspace. In turn, they are severely criticized and questioned by some sections of civil society who, on the contrary, highlight the usefulness of these spaces where anonymity is relatively preserved for journalists or dissidents threatened by authoritarian regimes, thus allowing the free flow of information and freedom of expression. However, States are also using the capabilities offered by darknets to create a new form of interstate or asymmetrical conflict for themselves, that is now taking place in virtual space, but has very severe consequences in the form of cyber-attacks, such as the large-scale one that took place in Estonia in 2007, inaugurating the entry into a new dimension of modern warfare. While, according to journalist Duncan Campbell [CAM 07], States have been losing the battle of cryptography to prevent the spread of advanced encryption techniques in civil society since the 1990s, it seems that Tor-like encrypted networks now offer capabilities to resist cyber-attacks and are also of interest to States and companies wishing to better protect their online databases.

The author of this book does not intend to propose a detailed technical approach of the different protocols and applications related to darknet here [REN 16]. It is not a computer manual either. The objective here is to deliver the keys to understanding a rapidly expanding phenomenon by defining the notions of the darknet, dark web and deep web by paying attention to the intellectual and ideological production that has accompanied and still accompanies the rise of alternative networks, in addition to examining the economic, security and geopolitical issues that are linked to the darknet (or deep web). Particularly, we will try to show that the clash between these different issues and between the diverging interests of users, institutions and economic operators always refers to the question of Internet governance modes. The darknets are on the threshold of a much more important era of development and make these questions crucial today because, as Peter Biddle, Paul England, Marcus Peinado and Bryan Willman asserted in 2003, “the genius of the darknet is indelible”.