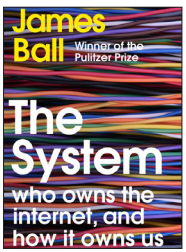
Australian Journal of Defence and Strategic Studies

Volume 2, Number 1 (2020)

ISSN 2652-3728 (PRINT) 2652-3736 (ONLINE)

https://www.defence.gov.au/ADC/Publications/AJDSS

Review: The System by James Ball



Reviewed by Tom Uren

To cite this article: Tom Uren, 'Review: The System: Who owns the internet, and how it owns us, review of The System: Who owns the internet, and how it owns us by James Ball, *Australian Journal of Defence and Strategic Studies* 2, 1 (2020): 149–154, http://www.defence.gov.au/ADC/publications/AJDSS/volume2-issue1/review3-the-system-james-ball.asp

Published online: 7 July 2020

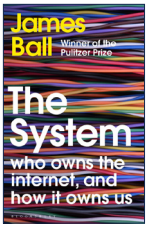
ADC Publications
Centre for Defence Research
Australian Defence College
PO Box 7917
CANBERRA BC ACT 2610
P: + 61 02 6266 0352
E: cdr.publications@defence.gov.au
W: defence.gov.au/ADC/publications/AJDSS

The System: Who owns the internet, and how it owns us

James Ball

Bloomsbury Publishing (August 2020)

Reviewed by Tom Uren



Left unchecked, the internet is a monopoly-making machine that elites are using to gather more wealth and power. This is the conclusion of James Ball, an accomplished author and Pulitzer prize winning journalist, formerly of the *Washington Post, WikiLeaks* and *The Guardian* (where he was involved with the Snowden leaks), in his recently published book The System, an ambitious attempt to write an unauthorised biography of the internet.

At its best the book educates and entertains with illuminating, well told stories about poorly understood corners of the internet: how it was created; how it is run; how new companies are financed through venture capital; and its darker aspects like user tracking and the world of targeted advertising. These stories lay bare the underlying incentives that exist online and shape behaviour. But ultimately, this book fails to weave Ball's many varied strands together into an entirely compelling argument.

The creation of the internet

Ball describes in broad strokes the very beginnings of the internet in the ARPANET project, funded by the Advanced Research Projects Agency (ARPA) of the Department of Defense (DoD).

ARPANET involved three factions collaborating: ARPA, who wanted new communication technologies for military command and control; university research scientists, who wanted to be able to use the massively expensive computers of the 1960s more efficiently; and a selection of young graduate students who actually built the protocols and technologies of the internet.

During this embryonic time, it was, ironically, the paths not taken and the decisions not made that have defined the character of the modern internet.

This first non-decision was project management. Although ARPA (and therefore DoD) ultimately provided funding for the project, it didn't manage the project in a hands-on way. Stakeholders across the three factions collaborated, but none were in charge. Given so much of the development work was done by relatively junior staff who felt they lacked hier-

archical authority, a culture was built around collaborative multi-stakeholder control. This paradigm endures to this day in the management and governance of the internet—all the organisations involved are collaborative and consensus-based.

Being government funded there was no requirement to recoup costs, so a second key non-decision was to not build a billing system to charge users. This meant that voice, video, audio and files were all just bits that were transmitted regardless. In-built billing would have resulted in telecommunications and ISP companies stifling innovation, through differential pricing, and placed them in a gatekeeper role, where they could have dictated terms for internet access. The lack of a billing mechanism has allowed an explosion of businesses to flourish and resulted in the tremendous proliferation of new apps as computers, smartphones and telecommunications became faster and more capable.

Perhaps the most consequential non-decision, at least from a national security point of view, was to not build ARPANET with a focus on security and identity. This made perfect sense in the context of a network of trusted researchers that were focused on solving the immediate problem of how to create a network of computers.

Although ARPANET was initially a research project it evolved and grew into what we now call the internet, and these key non-decisions still shape the internet of today.

Fifty years later, collaborative multi-stakeholder cooperation is still the model for internet governance. Ball explores how the organisation responsible for managing the internet's naming system operates, the Internet Corporation for Assigned Names and Numbers (ICANN). The costs of the consultative multi-stakeholder model of governance is in full view. Despite pressing security flaws in key internet protocols improvement happens at an agonisingly slow pace.

ICANN has technical expertise but because of its governance model no political agenda, no clout and no capacity for implementing it even if it did have one. Change only occurs when many different stakeholders with different motivations can agree. This conservatism has at least one significant benefit—it is difficult for ICANN to be captured to benefit malign actors.

Venture capital and financing

After tackling the origins and management of the internet, Ball explores how internet companies are financed through venture capital (VC), providing a short introduction to the VC industry and describing the perverse incentives that result from this financing model.

The Silicon Valley venture capital world, as Ball describes it, is a circle.

People who have made boatloads of money from fast-growing global internet businesses are well placed to then make early-stage investments in other fledgling fast-growing global internet businesses.

The expectations of investors coupled with the possibility of massively profitable global internet businesses results in start-ups that consume cash to grow fast, building 'minimum viable products' without thought of the broader consequences. That these companies often don't consider the ways that their technologies can be abused is exemplified by a former Facebook motto: 'move fast and break things'. Ball reports that Mark Zuckerberg, CEO of Facebook, initially found it inconceivable that Facebook would be manipulated in an attempt to steal an election, an amazingly naïve position given the years of Russian effort to stoke division and influence in American audiences.

In addition to contending that the VC system entrenches and centralises power in a wealthy elite, Ball also examines how power has accrued to a handful of extremely large technology companies such as Google, Facebook and Amazon. He relays interviews from venture capitalists who argue that cookies, which started as small text files to keep track of interactions with websites, enabled the tracking that has so empowered these large companies.

In chapter five, the most interesting part of the book, Ball also examines the targeted advertising businesses that operate behind the scenes on the web. These businesses hold auctions, within fractions of a second, for the opportunity to advertise to you whenever you visit a website. Data is exchanged and gathered to determine what sort of user you are and what you are after—so buyers can determine how much to pay for you.

Rather than helping quality publishers achieve higher ad rates and earn more revenue, Ball's interviewees argue that the effectiveness of tracking has allowed the opposite to occur *The New York Times* site, for example, runs nine different tracking services that aim to track your movements across the web. But rather than paying top dollar to advertise on the *Times* website to reach a reader, an advertiser can target that exact same reader on a lower quality and therefore cheaper website. Certainly, the data is irrefutable—advertising money has disappeared from traditional publications and migrated towards Facebook and Google.

The weakest section of the book deals with state espionage and cyber operations and this is where Ball's tendency to reflexively blame Western intelligence agencies for the internet's poor cyber security shines through. Ball primarily discusses the activities of US and UK intelligence agencies, relying heavily on the Snowden dis-

closures, and (ironically, for a book that emphasises the system of incentives on the internet) holds Western intelligence agencies responsible for the bad behaviour of foreign intelligence services.

For example, Ball discusses the 'WannaCry' ransomware attack, a destructive hard disk wiping attack launched by the North Korean government, but he focuses blame mainly on the US intelligence community because a sophisticated software capability was stolen from them and used in the construction of the WannaCry malware. It is a complex tale, and certainly the US government deserves *some* blame, but a balanced discussion would also examine the motives of those who stole the code and posted it to the internet as well as the motives of the North Koreans themselves.

Destructive attacks, state interference in democratic elections, rampant espionage and intellectual property theft—certainly there is much to dislike about the current state of play in state cyber operations. But this all stems from the third non-decision in the early days of the internet, to not incorporate robust security into internet protocols.

Much of the online behaviour that Ball describes has the feeling of inevitability. For instance, it was probably inevitable, given the increasing availability and sensitivity of information online, that intelligence agencies the world over would seek to gather intelligence through the internet. It is where valuable intelligence is. And, this is not new. Clifford Stoll, in his 1989 book, *The Cuckoo's Egg*, describes his quest to capture a hacker who was breaking into the Lawrence Berkeley National Laboratory computer systems to extract military secrets on behalf on the KGB.[1] Chinese hackers have been operating to steal intellectual property since the early 2000s. Despite Ball's assertion, foreign intelligence agencies did not need the 2013 Snowden revelations to justify their own behaviour online. Intelligence agencies have probably been among the first government entities to understand the internet—from the narrow perspective of intelligence collection—because they have been among the first forced to migrate online.

Similarly, the underlying economics of online businesses has also, perhaps inevitably, encouraged the growth-at-all-costs behaviour Bell describes. Upfront costs to build online businesses are large, but the marginal costs for additional clients are very low. Coupled with this, many online businesses exhibit what are called 'network effects' and become more valuable the more users they have. Facebook, for example, is valuable

1 Cliff Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Reissue edition (New York: Gallery Books, 2005).

because your friends and family are there—more users on Facebook makes it more valuable to more people. In the absence of a social network layer built into the fabric of the internet, it seems inevitable that an aggressive grow-at-all-costs company would come to dominate social networking, while making numerous missteps.

In other words, Ball too often reverses causality. Groups behave badly on the internet because of the incentives that the internet provides, incentives that often stem from the early non-decisions, especially regarding security, billing and collaborative decision-making. Supporting systems coalesce around these incentives to reinforce or reject them: venture capitalists, advertising and tracking industries, intelligence agencies, regulators and advocates.

Ball also seems to overestimate the capacity of governments to understand and rationally respond to the changes that the internet has brought. Governments still struggle to conceptualise how online businesses differ from traditional ones, and decisions have not been made recklessly or with wilful blindness—they've been taken in ignorance. Just as the early creators of the internet could not forecast the ramifications of some of their early non-decisions, government regulators don't yet have the understanding and frameworks to know how to make sensible decisions.

Ball raises the possibility that Chinese internet giants will have more influence over the future internet, but it is worse than that. There is now a clear and present danger to the internet's current governance models. The Chinese government is seeking to dominate global networks and platforms by influencing standards—'China Standards 2035'.[2] Huawei has already proposed a 'New IP' protocol that reportedly allows more centralised control[3], and the Chinese government is certainly seeking to mould the internet in its favour.

Ball's solution to the internet's problems is to, firstly, recognise and understand the problem, and secondly to look for lots of small fixes: protecting and valuing personal data; taxing multinationals; tackling bias; encouraging transparency; and improving security.

2 Emily de La Bruyère and Nathan Picarsic, 'China's next Plan to Dominate International Tech Standards', *TechCrunch*, 12 April, 2020, https://social.techcrunch.com/2020/04/11/chinas-next-plan-to-dominate-international-tech-standards/ .

3 Madhumita Murgia and Anna Gross, 'China and Huawei Propose Reinvention of the Internet', *Financial Times*, 4 May 2020, https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2 .

The internet has grown organically and to some extent reflects the libertarian ideals so eloquently captured in '*A Declaration of the Independence of Cyberspace*':[4]

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

Now, however, there is a competing vision, an internet modified to suit the needs of authoritarian states that quash dissent. For several years, Australia and other Western nations have been promoting a 'free, open and secure' internet. We need to decide, at a detailed technical level what that actually means and engage with internet governance bodies to promote that future.

This may mean re-examining the close relationship between our national intelligence and information security apparatus. Guilt-by-association from the Snowden disclosures may make it difficult for our national information security authorities to have influence in sceptical multi-stakeholder organisations if mixed motives are suspected, making it difficult to advance much needed security improvements.

To manage the future development of the internet we need to truly understand how the internet operates and the incentives it provides to businesses, governments and citizens. This book goes part way and sheds light but not always understanding.

4 John Perry Barlow, A Declaration of the Independence of Cyberspace (Davos, 1996) available via the John Perry Barlow Library, Electronic Frontier Foundation, see https://www.eff.org/cyberspace-independence