Shadowboxing: The Data Shadows of Cold War International Law

FLEUR JOHNS

(2017) Forthcoming in Matthew Craven, Sundhya Pahuja, Gerry Simpson and Anna Saunders (eds), *Cold War International Law*
[2017] *UNSWLRS* 62

UNSW Law
UNSW Sydney NSW 2052 Australia

Draft of 4 September 2017
Forthcoming in Matthew Craven, Sundhya Pahuja, Gerry Simpson and Anna Saunders (eds), *Cold War International Law*.

Shadowboxing:

The Data Shadows of Cold War International Law

Fleur Johns

Abstract

That states have come to be represented in "data shadows" for international legal purposes – that is, that state populations' condition may be gleaned from remotely sensed data to overcome deficiencies in official government statistics – is today identified with digital innovation. "Data shadows" were, however, crucial features of Cold War international law. Cold War decision-makers were captivated by the prognostications and intimations of "sigint" (signals intelligence). International legal order came to be marked, during the Cold War, by the latent or virtual agency of states' sigint data shadows in ways that leave an enduring legacy today.

Keywords: International law, technology, Cold War, signals intelligence

I Introduction

In recent years, states have come to be represented in 'data shadows' for international legal purposes. That is, the economic, social and political conditions of state populations captured in public-private assemblages of digital data (designed to overlay, and overcome deficiencies in, official government statistics) have been rendered actionable for a wide range of law and policy purposes.[1] This means that the agency with which any one state is invested in the global legal order, and the conduct and views ascribed to it by other agents for legal and political purposes, will often emerge from the combined effect of multiple avatars of that state circulating in public or private data,

[1] Shelton et al, 'Mapping the Data Shadows of Hurricane Sandy: Uncovering the Sociospatial Dimensions of "Big Data"'(2014) 52 *Geoforum* 167; Linnet Taylor and Dennis Broeders, 'In the Name of Development: Power, Profit and the Datafication of the Global South' (2015) 64(4) *Geoforum* 229; Fleur Johns, 'Data Territories: Changing Architectures of Association in International Law' (2016) 47 *Netherlands Yearbook of International Law* (forthcoming) <https://ssrn.com/abstract=2810897>.

or combinations of the two. Moreover, the composite characteristics of this multivalent state may be within only partial purview of leaders and policymakers in the state in question, belying the notion of international law as determined by the rationally expressed views and interests of sovereign elites. That this is the case could be identified with quite recent innovations in digital technology, on one hand, and the post-1989 rise of non-state actors and mediators in international legal affairs, on the other.[2] In this chapter, however, I will suggest that 'data shadows' of this kind were already crucial features of Cold War international law.

During an era marked by suspicion, and recurrent failures of 'humint' (human intelligence gathering), Cold War decision-makers were increasingly captivated and guided by the prognostications and intimations of 'sigint' (signals intelligence), 'comint' (communications intelligence), and 'elint' (electronic intelligence): that is, intelligence gathering through the interception and interpretation of electronic or electromagnetic signals and communications.[3] Decision- and policy-making under the rubric of international law engaged continually with the would-be, could-be or might-have-been moves of key protagonists, as those moves appeared in electronic data. International legal order came to be marked, during the Cold War, by the latent or virtual agency of these overlapping data shadows in ways that leave an enduring legacy today. This is demonstrated here by brief discussion of two instances of international

[2] On the first factor, see, e.g., Mark Graham, 'Internet Geographies: Data Shadows and Digital Divisions of Labour' in: Mark Graham and William H Dutton (eds), *Society and the Internet: How Networks of Information and Communication Are Changing Our Lives* (Oxford University Press, 2014) 99. On the second, see generally Rainer Hofmann (ed), *Non-State Actors as New Subjects of International Law* (Duncker & Humblot, 1998).

[3] Matthew M Aid and Cees Wiebes (eds), *Secrets of Signals Intelligence During the Cold War and Beyond* (Frank Cass, 1st ed, 2001) 2-3; Matthew M Aid and Cees Wiebes, 'Introduction on The Importance of Signals Intelligence in the Cold War' (2001) 16(1) *Intelligence and National Security* 1. On the prevalence of suspicion, see Stephen J Whitfield, *The Culture of the Cold War* (John Hopkins University Press, 2nd ed, 1996).

conflict, and associated legal analysis, in 'the 'hottest' theatre' of the Cold War: Asia.[4] The two instances in question are the Tonkin Gulf incidents of 2nd and 4th August 1964, between the United States of America and North Vietnam, and US prediction and detection of China's testing of that nation's first fission nuclear bomb at Lop Nur on 16th October 1964.[5]

In the second and third parts of this chapter, I will outline – briefly and selectively – some of the basic infrastructure of Cold War signals intelligence on which the generation and circulation of data shadows surrounding these incidents depended: first, in its technical, and later, in its legal dimensions. I will then turn to the two instances just mentioned in which a data shadow of an Asian communist nation loomed especially large in the sightlines of the US and its allies. I will conclude with a brief reflection on some ramifications of data shadows' prevalence in Cold War international law and their enduring salience for contemporary international law and lawyers.

[4] Richard J Aldrich, Gary D Rawnsley & Ming-Yeh T Rawnsley (1999) 'Introduction: The Clandestine Cold War in Asia, 1945–65' (1999) 14(4) *Intelligence and National Security* 1, 1.
[5] Edwin E Moïse, *Tonkin Gulf and the Escalation of the Vietnam War* (University of North Carolina Press, 1996); William Burr and Jeffrey T Richelson, 'Whether to Strangle the Baby in the Cradle: The United States and the Chinese Nuclear Program, 1960-1964' (2000/01) 25(3) *International Security* 54.

II The Technical infrastructure of Cold War Signals Intelligence

In order to grasp how the international legal order came to animate and be animated by data shadows during the Cold War, it is important to understand something of the technical capacities that states acquired and deployed throughout this period for capturing or envisioning the actions (or potential actions) of their adversaries electronically. Some of these capacities vested in private and intergovernmental actors as well, or depended on their mediation. This section provides a brief overview of some of the technical infrastructure and capabilities built up over the course of the Cold War that enabled states, in particular, to generate and engage with spectral versions of each other rendered in data. By reason of the relative accessibility of information about them, I will focus on Cold War capabilities on the US-aligned side.

Among the forms of electronic data in which states' actions and intentions were readable during the Cold War was the ciphered cablegram, used to convey messages among diplomatic and intelligence personnel. This was an electrical telegraph sent by subterranean and submarine cable and, in diplomatic and intelligence contexts, encrypted using a ciphering system to ensure inaccessibility to all but intended recipients. During the Cold War era, however, advancements in (human, rather than automated) code-breaking technique enabled this cable traffic to be read by adversaries seeking evidence of the conduct and plans of the states concerned, such that these electronic data were called upon to cast shadows of a state's intentions and machinations. In 1943, for example, acting on concern about the prospect of a second Nazi-Soviet Pact, the US Army's Signals Intelligence Service began a small program

to decipher Soviet diplomatic cables code-named 'Venona'.[6] By 1948, under the rubric of this program, US codebreakers were reading Russian diplomatic, military, naval, and police traffic in several cryptosystems.[7] Data decrypted through the Venona program became crucial to the FBI, and to its counterparts in allied states, identifying the presence and tracking the operations of Soviet spy rings throughout the 1950s; these data permitted the US and its close allies to follow and act on the electrical slipstream of Soviet statecraft.[8]

A second data source that became significant during the Cold War, and a further setting for the electronic projection and gathering of information about states' conduct and plans, was intercepted radio traffic (that is, the interception of electromagnetic energy waves modulated to transmit information). Between 1950 and 1960, the US National Security Agency (NSA) and Central Intelligence Agency (CIA) constructed a network of some seventy strategic intercept stations, and about an equal number of tactical communication intelligence units, around the world.[9] This network operated in tandem with approximately thirty-five radio intercept stations operated by Britain, Canada, Australia and New Zealand: the US' four treaty partners under the UKUSA Agreement

[6] Ruud van Dijk et al (eds), *Encyclopedia of the Cold War* (Routledge, 2008) 940; John Ferris, 'Signals Intelligence in War and Power Politics, 1914-2010' in Loch K Johnson, *The Oxford Handbook of National Security Intelligence* (Oxford University Press, 2010) 155, 168 citing David Alvarez, *Secret Messages: Codebreaking and American Diplomacy, 1930–1945* (University Press of Kansas, 2000); R L Benson and M Warner (eds), *VENONA: Soviet Espionage and the American Response, 1939–1957* (CIA/NSA, 1996); Christopher Andrew, 'Intelligence in the Cold War' in M Leffler & O Westad (eds), *The Cambridge History of the Cold War* (Cambridge University Press, 2010), vol 2, 417, 418-19.
[7] David Alvarez, 'Behind Venona: American Signals Intelligence in The Early Cold War' (1999) 14(2) *Intelligence and National Security* 179, 180.
[8] Matthew M Aid, 'The National Security Agency and the Cold War' (2001) 16(1) *Intelligence and National Security* 27, 40. For information regarding impact on Australian intelligence see: Christopher Andrew, 'The Growth of the Australian Intelligence Community and the Anglo-American Connection' (1989) 4(2) *Intelligence and National Security* 213, 227.
[9] Aid, 'The national Security Agency and the Cold War', above n 8, 36; Jeffrey T Richelson, *The CIA and Signals Intelligence: Electronic Briefing Book No. 506* (20 March 2015) National Security Archive <http://nsarchive.gwu.edu/NSAEBB/NSAEBB506/> citing Jeffrey T Richelson, *The Wizards of Langley: Inside the CIA's Directorate of Science and Technology* (Westview, 1st ed, 2001) 33, 88.

known as the 'Five Eyes' arrangement (discussed further below).[10] Their interaction permitted the interception and copying of shortwave radio traffic transmitted from within the periphery of the Soviet Union, and from Eastern Europe, China and North Korea.[11] Throughout this decade, NSA intercept operators stationed around the world spent most of their time monitoring and transcribing radio traffic concerning the day-to-day routine activities at foreign military bases.[12]

During the 1960s, high frequency radio detection and interception infrastructure became more elaborate and integrated. A worldwide high frequency radio detection and signals intelligence system (initially called 'Classic Bullseye') combined and strengthened the sigint capacities of the 'Five Eyes' states. This was comprised of an automated network of circular antennae arrays designed to detect radio signals from aircraft or ships; calculate the direction, or line of bearing, of the radio transmitter; and thereby enable the interception of communications traffic transmitted on short-wave channels.[13]

[10] The UKUSA Security Agreement on communications intelligence cooperation comprises a still-classified set of memoranda of understanding and exchange of letters negotiated between the US and UK in the 1946-48 period and signed in 1948 among those two countries, Australia, Canada and New Zealand, to constitute an arrangement known as the 'Five Eyes'. Subsequent bilateral arrangements added a range of participating 'Third Parties', including Sweden and Norway. See Martin Rudner, 'Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism' (2004) 17(2) *International Journal of Intelligence and Counterintelligence* 193, 197, 224 (see footnotes 4-6); Christopher Andrew, 'The Making of the Anglo-American SIGINT Alliance' in Hayden Peake and Samuel Halpern (eds), *In the Name of Intelligence: Essays in Honor of Walter Pforzheimer* (NIBC Press, 1994) 95.

[11] Aid, 'The National Security Agency and the Cold War', above n 8, 36.

[12] Aid and Wiebes, 'Introduction on The Importance of Signals Intelligence in the Cold War', above n 3, 3.

[13] Matthew M Aid, 'The National Security Agency and the Cold War', in Matthew M Aid & Cees Wibes (eds), *Secrets of Signals Intelligence During the Cold War and Beyond* (Frank Cass, 1st ed, 2001) 27, 45; Federation of Atomic Scientists, Intelligence Resource Program, *AN/FRD-10 Classic Bullseye* (26 November 2001) <https://fas.org/irp/program/collect/classic_bullseye.htm> (last visited 7 July 2017).

During the 1950s and 1960s, also, this US-backed sigint capacity went mobile. US navy warships began to be fitted for secure communication and to double as remote intelligence-gathering platforms.[14] In Asia especially, so-called DESOTO patrols (DEHAVEN Special Operations Off Tsingtao) were conducted by US navy destroyers equipped with mobile signals intelligence-gathering capacity in the South China Sea and throughout the Tonkin Gulf.[15] The U2 aerial reconnaissance aeroplane and related overflight program was introduced in 1956, although it was plagued by problems.[16] Even so, by the late 1950s, sigint and U-2 imagery were widely deemed to be the most credible and productive sources of 'hard intelligence' about the Soviet Union and Warsaw Pact countries.[17]

Other Western nations collaborated in the deployment of mobile, remote detection and data-gathering capacities during the same period. In the early-to-mid-1950s, for example, the Swedish Defence Research Establishment known as the FOA was flying

[14] Michael Warner, 'The Rise of The US Intelligence System, 1917-1977' in Loch K Johnson (ed), *The Oxford Handbook of National Security Intelligence* (Oxford University Press, 2010) 107, 114 citing C Ford and D Rosenberg, 'The Naval Intelligence Underpinnings of Reagan's Maritime Strategy' (2005) 28 *Journal of Strategic Studies* 380; see also Wyman H Packard, *A Century of US Naval Intelligence* (Office of Naval Intelligence and Naval Historical Center, 1996).

[15] National Security Agency, *United States Cryptologic History*: *American Cryptology during the Cold War, 1945-1989: Book II – Centralization Wins, 1960-1972* (13 February 2006) 515-516, <https://www.nsa.gov/news-features/declassified-documents/gulf-of-tonkin/articles/assets/files/release-2/rel2_american_cryptology.pdf>; National Cryptologic School, *Chapter Six: The Gulf of Tonkin Incident: The DESOTO Patrols and OPLAN 34A* (20 December 2005) National Security Agency, <https://www.nsa.gov/news-features/declassified-documents/gulf-of-tonkin/articles/assets/files/release-2/rel2_gulf_tonkin_incident_desoto.pdf>; see further NSA, *Articles about the Gulf of Tonkin Events* (3 May 2016) <https://www.nsa.gov/news-features/declassified-documents/gulf-of-tonkin/articles/release-2.shtml>.

[16] Gregory W Pedlow and Donald E Welzenbach, *The CIA and the U-2 Program, 1954-1974* (History Staff Center for the Study of Intelligence, CIA, 1998) <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/the-cia-and-the-u-2-program-1954-1974/u2.pdf>; Dino Brugioni, *Eyes in the Sky: Eisenhower, the CIA, and Cold War Aerial Espionage* (Naval Institute Press, 2010) (see ch 8 'The U-2 Missions Begin'; ch 11 'The U-2 Flights Resume'; ch 12 'Tactical use of the U-2 and Related Technical Developments'); Chris Pocock, *50 Years of the U-2: The Complete Illustrated History of the "Dragon Lady"* (Schiffer Publishing, 2005); Jeffrey T Richelson, *The Secret History of the U-2 — and Area 51: Electronic Briefing Book No. 434* (15 August 2013) National Security Archive <http://nsarchive.gwu.edu/NSAEBB/NSAEBB434/>.

[17] Aid, 'The National Security Agency and the Cold War', above n 8 40; Warner, above n 14, 115; Andrew, above n 6, 421.

DC-3 Dakota aircraft (also designated TP-79) equipped with electronic intelligence collection equipment provided by the US.[18] In 1953, after the loss of the Dakota, Sweden purchased a British TP-82 Varsity which performed covert electronic data collection missions over the Baltic until 1973.[19]

Remote, automated reconnaissance and mobile sigint infrastructure entered a further, revolutionary phase with the Soviet Union's October 1957 launch into orbit of Sputnik, the world's first satellite of human manufacture.[20] Shortly afterwards, in 1958, the US launched Project SCORE (Signal Communications by Orbiting Relay Equipment), to demonstrate the feasibility and refine the operation of satellite communications.[21] This was soon followed by the US launch of operational satellites Echo 1 (the first passive communications satellite), in 1960, and Telstar 1 (the first electronic communications satellite) in 1962.[22] 1960 also saw the US successfully launch the Discoverer 13 – the world's first, operational reconnaissance satellite – as part of a classified program aimed at developing film-return photographic satellite surveillance capacity to assess Soviet progress in producing and deploying long-range bombers and ballistic missiles and take aerial reconnaissance photographs across Sino-Soviet territory (in place of the U2 spy planes).[23] Between 1968 and 1989, the US went on to launch several successive

[18] Alf R Jacobsen, 'Scandinavia, Sigint and the Cold War' (2001) 16(1) *Intelligence and National Security* 209, 223.
[19] Ibid 234.
[20] George Reisch, 'When Structure Met Sputnik: On the Cold War Origins of the Structure of Scientific Revolutions' in Naomi Oreskes & John Krige, *Science and Technology in the Global Cold War* (MIT Press, 2014) 372, 372; van Dijk et al (eds), above n 6, 770.
[21] *Score* (21 March 2017) NASA Space Science Data Coordinated Archive, <https://nssdc.gsfc.nasa.gov/nmc/spacecraftDisplay.do?id=1958-006A> (last accessed 7 July 2017).
[22] Van Dijk et al (eds), above n 6, 770; Donald C Elder, 'Something of Value: Echo and the Beginnings of Satellite Communications', in A J Butrica (ed), *Beyond The Ionosphere: Fifty Years of Satellite Communication* (NASA History Office, 1997), available at https://history.nasa.gov/SP-4217/ch4.htm (last accessed 7 July 2017).
[23] *Discoverer 13* (21 March 2017) NASA Space Science Data Coordinated Archive, https://nssdc.gsfc.nasa.gov/nmc/spacecraftDisplay.do?id=1960-008A (last accessed 7 July 2017); van Dijk et al (eds), above n 6, 770.

generations of satellites dedicated to signals intelligence, electronic intelligence and/or the interception and analysis of communications.[24] Pursuant to the UKUSA Agreement and its derivatives, all 'Five Eyes' participants were able to access and share among themselves the products of this satellite interception infrastructure.[25]

The development of satellite communications and networking technologies from the late 1960s onwards presented new opportunities for global collaboration in the gathering, processing and sharing of intelligence data. By the early 1970s, this included early versions of the networking and processing software that came to be known as ECHELON, enabling intercept stations (that is, ground stations, together with facilities for monitoring microwave and cable transmissions) operated by the various UKUSA Agreement participants to form 'an integrated, virtually seamless SIGINT interception and processing network' spanning the globe and extending to messages sent via satellite [26] During the last decades of the Cold War, the volume and range of communications to which this surveillance network could extend increased exponentially upon the introduction of computer networks linked via packet-switching technology (beginning with the US Defense Department's Advanced Research Projects Agency Network, or ARPANET) and the development of the transmission control protocol (TCP) and Internet protocol (IP) (typically referred to as TCP/IP). Together,

[24] Martin Rudner, 'Canada's Communications Security Establishment from Cold War to Globalization', in Matthew M Aid & Cees Wibes (eds), *Secrets of Signals Intelligence During the Cold War and Beyond* (Frank Cass, 1st ed, 2001) 97, 109-10; Loch K Johnson, *Secret Agencies: US Intelligence in A Hostile World* (Yale University Press, 1996) 178.
[25] Rudner, 'Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism' above n 10, 200-1.
[26] Ibid 201. See also Gerhard Schmid, *Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System) (2001/2098(INI))* Eur. Parl. Doc. A5-0264/2001 (11 July 2001) 67-72, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN> (last accessed 7 July 2017).

these enabled the multi-host, high-speed communications characteristic of the Internet; by 1987 there were already some 30,000 hosts on the Internet.[27]

As much as it ever emanated from minds, mouths and meeting rooms in the metropolitan centres of major players in the Cold War, the era's legal and political relations were thus the product of the growth and confluence of these physical and technological infrastructures and of the electronic projections of conduct and communication that they carried and produced. Cold War era treaty drafting focused on deliberative processes arising from or occasioning some high-level meeting of minds. The 1969 *Revised American-Soviet Draft Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Sea-Bed and the Ocean Floor and in the Subsoil thereof*, for example, aimed to foster 'consult[ation] and cooperat[ion] with a view to removing doubts concerning the fulfillment of… obligations assumed'.[28] At the same time, however, doubts about the reach of human relations and the power of human insight were being both addressed and intensified by advances in intelligence infrastructure and the suggestive and multiple data shadows that it cast on either side of the Iron Curtain.

The Cold War may have produced, as David Kennedy has observed, 'institutional terrain for global political conversation that crisscrosses governments, corporations, and civil society' in search of a 'common language of engagement' and convergence of values.[29] Yet the Cold War also produced and relied upon terrain for global

[27] Byung-Keun Kim, *Internationalizing the Internet: The Co-evolution of Influence and Technology* (Edward Elgar Publishing, 2005) 51-5; Johnny Ryan, *A History of the Internet and the Digital Future* (Reaktion Books, 2010) 11-22.
[28] CCD/269/Rev. 1, draft as at 30 October 1969 <https://2001-2009.state.gov/r/pa/ho/frus/nixon/e2/83553.htm> (last accessed 7 July 2017).
[29] David Kennedy, *A World of Struggle: How Power, Law, and Expertise Shape Global Political Economy* (Princeton University Press, 2016) 222.

interaction that was neither conversational in character, nor necessarily predicated upon the search for or mobilization of a 'common language' or contingent on much by way of value-convergence among humans. That interaction was comprised of the ever-intensifying whirrings, beeps, and tics of the global infrastructure just described, the protocols and patterns structuring its operations, and the human-nonhuman interpretation of its emissions.

The hybrid outputs of the latter infrastructure presented Cold War decision-makers with auguries of state conduct and intent that travelled alongside those generated by conventional 'political conversation[s]' and diplomatic protocols, perpetually shadowing, and sometimes disjoining or second-guessing the latter. This rise to prominence, in global legal and political affairs, of spectral data doubles followed on the heels of a revival of popular occultism that occurred during the Second World War and lingered in its aftermath.[30] In 1944, for instance, the *New York Times* reported that US popular culture was 'haunted as never before […] [as] an odd sort of escape from a world in which evil and terror are, objectively, literally, so important, but not unexpected'.[31] This occultist fixation echoed preoccupations that a further spectral object engendered in the West throughout the Cold War – namely, the latent presence of Communism. This was the 'spectre' which Marx and Engels had announced to be 'haunting Europe' already in 1848.[32] As such, Cold War data shadows served to

[30] Tim Snelson, 'The Ghost in the Machine', (2011) 17 *Media History* 17. See also Cynthia Hendershot, *I Was a Cold War Monster: Horror Films, Eroticism, and the Cold War Imagination* (Popular Press, 2001).
[31] Norman Matson, 'Gooseflesh Special', *New York Times* (New York) 28 May 1944, 7, quoted in Snelson, ibid.
[32] Karl Marx and Friedrich Engels, 'The Manifesto of the Communist Party' in Robert C Tucker (ed), *The Marx-Engels Reader* (2nd ed., W.W. Norton & Co., 1978) 469, 473 ('A spectre is haunting Europe – the spectre of Communism').

amplify a global atmosphere of suspicion and anxiety characteristic of the period, at least in the West.

III The Legal infrastructure of Cold War Signals Intelligence

Alongside, and in interaction with, the technical developments outlined in the preceding section there emerged, over the course of the Cold War, a legal infrastructure that enabled the production and circulation of data shadows – namely, the legal infrastructure surrounding the collection and sharing of signals intelligence across national borders. It is common to frame global intelligence-gathering and -sharing as a political expression of state sovereignty – a practice that international law 'neither endorses nor prohibits' so much as 'preserves', tolerates or 'functionally permits', except in so far as it risks tripping international legal barriers of non-intervention and non-interference.[33] Yet international law maintains normative infrastructure enabling of these practices, and has done so since well before the Cold War.

A keystone of this normative architecture is the Constitution and Convention of the International Telecommunication Union (ITU), an instrument formerly known as the International Telecommunication Convention.[34] The ITU was established in 1932 by the Madrid Radiotelegraph Conference as a successor to the nineteenth century's International Telegraph Union and has, since 1947, been a specialised agency of the

[33] Christopher D Banker, 'Tolerance of International Espionage: A Functional Approach' (2004) 19 *American University International Law Review* 1091, 1092; Simon Chesterman, 'The Spy Who Came in from the Cold War: Intelligence and International Law' (2005-2006) 27 *Michigan Journal of International Law,* 1071, 1077, 1081-7.
[34] Anthony Rutkowski, 'International Signals Intelligence Law: Provisions and History' (2016) 4 *Lawfare Research Paper Series*, <https://www.lawfareblog.com/anthony-rutkowski-international-signals-intelligence-law-provisions-and-history-lawfare-research>.

United Nations.[35] The term 'telecommunication' in this context has always been defined expansively; the current version of the Constitution defines the term to mean '[a]ny transmission, emission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems'.[36]

Far from consigning sigint to the murky background of their discussions, the Member States of the 1932 Madrid Conference committed from the outset to the permissibility of private telecommunications' stoppage in the event of any transmission 'appear[ing] dangerous to the security of the State or contrary to its laws, to public order or to decency'.[37] To this day, Member States of the ITU are assured by Article 34 of the Constitution of the 'right to cut off' telecommunications in such circumstances 'in accordance with their national law'.[38] As such, this clause (and its predecessors dating back to the 1930s) made way for the maintenance of sigint interception and surveillance capabilities sufficient to detect the kinds of 'dangerous[ness]' that may trigger a right of stoppage.

In a similar vein, Article 37 of the Constitution (again, a clause that dates in some form from the earliest days of the organisation) requires ITU Member States to 'take all possible measures, compatible with the system of telecommunications used, with a view to ensuring the secrecy of international correspondence'. Nevertheless, the same

[35] Francis Colt de Wolf, 'Telecommunications in the New World' (1945-46) 55 *Yale Law Journal* 1281; Poul Hansen & William H Melody, 'The International Telecommunications Union at the Crossroads' (1989) 7(2) *Prometheus* 254.
[36] *Constitution and Convention of the International Telecommunication Union*, signed 22 December 1992, ISBN 92-61-04771-8 (entered into force 1 July 1994) annex, ¶1012, <http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.12.61.en.100.pdf>. (last accessed 7 July 2017).
[37] Rutkowski, above n 34, 4-5.
[38] *Constitution and Convention of the International Telecommunication Union*, signed and entered into force 7 November 2014, ISBN 978-92-61-14691-7, art 34.

Article provides – and has provided in some form since inception – for Member States to 'reserve the right to communicate such correspondence to the competent authorities in order to ensure the application of their national laws or the execution of international conventions to which they are a party'.[39] Once again, this presumes and affirms states maintaining capacity to intercept and redirect telecommunications, or decipher and divulge their contents, wherever necessary to meet the needs of law enforcement agencies and officials under applicable national or international laws.

A further set of long-maintained provisions in the Constitution provide for multi-party policing of the radio spectrum 'through mutual assistance, information sharing, and monitoring at both national and international levels'.[40] The clauses in question are known as the 'harmful interference clause' (Article 45, requiring Member States to take steps to prevent harmful interference to radio services or communications) and the 'infringements clause' (Article 39, in which Member States undertake to inform and assist one another with regard to infringements of the Constitution or Convention or corresponding administrative regulations). These are complemented by a clause (the 'monitoring clause') providing for cooperation in the establishment of an international system of frequency monitoring stations and their operation by a government administration, public or private enterprise, bilateral service or international organization (Article 16 of the ITU Radio Regulations).[41]

In this way, the ITU Constitution and Convention and related instruments have established an expectation – indeed, a legal obligation, to some degree – on the part of

[39] Ibid art 37.
[40] Rutkowski, above n 34, 7.
[41] International Telecommunication Union, *Radio Regulations* (1 January 2017) <http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/1.43.48.en.101.pdf>.

Member States to maintain, on their own part or in collaboration with others, communications and signals intelligence capabilities for the detection and prevention of prospects of harm to the infrastructure described in the preceding section. The maintenance of global telecommunications capability is cast in this context as an unquestionable imperative, and sigint characterised as essential to its defence.

Setting aside matters of national and comparative law, much of the remaining normative infrastructure that occasioned or shaped the circulation of data shadows on the global plane during the Cold War is difficult to map by reason of its non-public status. As noted above, the UKUSA Agreement (known as the 'Five Eyes' arrangement), concluded at the end of the Second World War and supplemented thereafter, remains classified; even its existence has only rarely been officially acknowledged.[42] According to '[a]vailable sources', this served throughout the Cold War as a 'framework mechanism for close collaboration between the United States and Great Britain, as First and Second Parties to the Agreement, in technology development, targeting and operations, and in the sharing of foreign intelligence products', with the one-time British territories (and additional Second Parties), Australia, Canada, and New Zealand remaining mostly 'at the periphery' of this collaboration.[43] Onto this framework many other allied agreements and partners were bolted over the course of the Cold War, conferring varying degrees of access and involvement in global intelligence-gathering, -processing and -sharing.[44]

[42] Rudner, 'Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism' above n 10, 197, 224 (note 6); Lawrence D Sloan, 'ECHELON and the Legal Restraints on Signals Intelligence: A Need for Reevaluation' (2001) 50 *Duke Law Journal* 1467, 1472.
[43] Rudner, 'Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism' above n 10, 193-230, 197.
[44] Ibid.

It may be the case that the 'successful collection of intelligence often requires violations of the law' – that is, both national and international law.[45] This chapter does not attempt any analysis of when, where or how, or under which laws, such violations may arise.[46] It may also be the case that the international law regulating sigint is – and was, during the Cold War – relatively 'underdeveloped', as many have suggested.[47] Nonetheless, this brief introduction to some of the international legal infrastructure underpinning Cold War era practices of sigint collection, analysis and distribution on the global plane makes apparent that the generation and circulation of data shadows in connection with these practices has been as much a result of compliance with or implementation of international law as defiance of it, or acting in its absence. In this sense, Cold War data shadows were techno-legal creations.[48]

IV **Cold War Data Shadows in the foreground: Tonkin Gulf and Lop Nur 1964**

Having introduced the phenomenon of data shadows as a noteworthy feature of Cold War international law, and identified two dimensions of the infrastructure supporting their generation and circulation, let us now consider two instances, both from 1964, in

[45] Sloan, above n 42, 1490.
[46] For examples of literature that does attempt such analysis, with varying emphases, see Sloan ibid; Craig Forcese, 'Spies without Borders: International Law and Intelligence Collection' (2011) 5 *Journal of National Security Law & Policy* 179; Craig Forcese, 'Pragmatism and Principle: Intelligence Agencies and International Law' (2016) 102 *Virginia Law Review* 67; Ido Kilovaty, 'World Wide Web of Exploitations - The Case of Peacetime Cyber Espionage Operations under International Law: Towards a Contextual Approach' (2016) 18 *Columbia Science and Technology Law Review* 42.
[47] Forcese, 'Spies without Borders: International Law and Intelligence Collection' above n 46, 185 quoting A John Radsan, 'The Unresolved Equation of Espionage and International Law' (2007) 28 *Michigan Journal of International Law* 595 and other sources.
[48] Framings of the 'techno-legal' as a target for inquiry abound in Science and Technology Studies research and legal research in dialogue with the same. See, e.g., Amit Prasad, 'Biopolitical Excess: Techno-Legal Assemblage of Stem Cell Research in India' (2017) 22(1) *Science, Technology & Society* 102. The conjunction suggestions the co-productive entanglement of technological and physical regimes and objects, on one hand, and legal regimes and objects, on the other (or in more traditional terms, the inextricability of the material and the ideal) and the importance of analyzing and critically engaging combined assemblages as such.

which data shadows played a critical role in Cold War international legal and political affairs; this will convey a sense of the ramifications of these data shadows' emergence. The first of these instances is known as the Tonkin Gulf affair. It concerned a series of confused military interactions between the US and North Vietnamese forces, and reverberations therefrom, that took place in August 1964. In these interactions, data shadows generated by US sigint infrastructure interacted, in perplexing and ultimately devastating ways, with the inputs and outputs of conventional national and international political and legal dialogue. Prompted by these interactions, on 7 August 1964, the two houses of US Congress passed what became known as the Tonkin Gulf Resolution affording US President Lyndon Johnson authority to take 'all necessary measures' to 'prevent further aggression' by North Vietnam. This became a key point of reference in the Johnson administration's later commitment of escalating numbers of US military forces to the Vietnam War.[49]

As alluded to above, in 1962, the US Navy commenced a covert sigint collection program centred on the fitting of DESOTO destroyer boats with direct support units for intelligence collection.[50] This included equipment to intercept both voice and manual Morse code communications, elint equipment (including radars), as well as equipment to send and receive communications to other monitoring stations and sigint processing and analysis sites. In their patrols of the Western Pacific, along the Asiatic coastline,

[49] Moïse, above n 5, xi, 226. See also Joseph C Goulden, *Truth is the First Casualty: The Gulf of Tonkin Affair – Illusion and Reality* (Rand McNally & Co., 1969); Joint Resolution to Promote the Maintenance of Peace and Security in Southeast Asia, HRJ Res 1145, 88th Congress (10 August 1964).
[50] Robert J Hanyok, *Spartans in Darkness: American SIGINT and the Indochina War, 1945-1975 – United States Cryptologic History: Series VI – The NSA Period 1952 – Present, Volume 7* (Center for Cryptologic History, National Security Agency, 2002) 175-230.

DESOTO boats both collected intelligence (covertly) and asserted freedom of navigation in international waters (overtly).[51]

In 1964, scheduled DESOTO patrols were requested to provide critical intelligence in support of a highly-classified program of covert actions that the US was preparing to launch against North Vietnam. The *USS Craig* carried out the first of the ensuing patrols in the Tonkin Gulf (off the coast of North Vietnam and southern China) in early 1964, prompting no reaction from the North Vietnamese.[52] The second such mission, for which the *USS Maddox* was deployed, entailed collecting intelligence on North Vietnam's coastal defense posture, by provoking and recording North Vietnamese reactions to US patrols.[53] As well as the naval detachment charged with sigint aboard the *Maddox*, this involved a US Marine sigint detachment located at the US Army base at Phu Bai in Central Vietnam and a US Marine sigint contingent at San Miguel in the Philippines. [54]

On the afternoon of 2 August 1964, *Maddox* detected three North Vietnamese torpedo boats approaching at high speed. In the face of this approach, *Maddox* was ordered to fire warning shots if they came closer than 10,000 yards. When the boats reached that point, *Maddox* fired three warning shots, but the torpedo boats continued at high speed. In the subsequent exchange of fire, neither US nor North Vietnamese ships suffered significant damage. [55] After this incident, *Maddox* resumed patrols on 3 August

[51] Ibid 178; Moïse, above n 5, 50-2; Goulden, above n 49, 104-110.
[52] Hanyok, above n 50, 178; Moïse, above n 5, 50.
[53] Hanyok, above n 50, 180.
[54] Hanyok, above n 50, 184; Moïse, above n 5, 52-5.
[55] Hanyok, above n 50, 190-192. Moïse, above n 5, 73-93.

accompanied by another destroyer the *USS Turner Joy*.[56] Late on the morning of 4 August 1964, the naval sigint detachment aboard the *Maddox* received messages from the US Marine sigint unit at Phu Bai suggesting that Vietnamese naval operations were planned against the DESOTO patrols. This 'significant error', and the flawed radar readings (or 'radar ghosts') on which it was based, coming fast on the heels of the 2 August attack, put the crew of the two US destroyers in mind that they would soon be attacked.[57]

Following detection of possibly hostile radar contacts earlier in the afternoon and evening, the night of 4 August saw the *Maddox* detect on its radar screens what was thought to be several boats in tight formation fifteen miles away from the vessel. The sudden appearance of a single boat on the *Maddox's* radar screen, east of the two destroyers and making a sharp turn, was interpreted as a turn after a torpedo run. A noise spike detected by the sonar operator aboard the *Maddox* was interpreted as a torpedo (although this was later to be determined to be a result of high-speed maneuvering by the two US ships).[58] In response to what was thought, on the basis of these confluence of errors, to be a Vietnamese torpedo attack, the US destroyers commenced firing on the supposedly attacking boats. After a period of minutes, the boats being tracked by the US destroyers disappeared from radar contact, but the two US destroyers nonetheless 'gyrated wildly in the dark … firing over 300 rounds madly at [what was thought to be] swarms of attacking North Vietnamese boats'.[59]

[56] Hanyok, above n 50, 195. Moïse, above n 5, 94-105.
[57] Hanyok, above n 50, 196, 222; Moïse, above n 5, 106-7, 112-3.
[58] Hanyok, above n 50, 196-8. See also Moïse above n 5, 106-142.
[59] Hanyok, above n 50, 197.

A later report commissioned by the NSA, finalised in 2002 but only made public in 2007, emphasized that sigint played a critical role in defining the second attack in the minds of Johnson administration officials. Without the sigint information, the administration had only confused and conflicting testimony of the men involved in the incident.[60] Some of those human witnesses 'developed doubts about the incident very quickly', but these had to contend with 'radar ghosts' and other suggestive data shadows generated by the transmission and interpretation of sigint. [61] The aforementioned NSA Report was to later observe that: '… it is not simply that there is a different story as to what happened [on the evening of 4 August 1964]; it is that *no attack* happened that night'.[62] That Report detailed how the representational effect of imprecise or inconclusive sigint data was compounded by analytic errors, the partial or decontextualized interpretation of data, and an unwillingness to consider contrary evidence, leading to profound misinterpretation of what was most likely a North Vietnamese navy operation to try to salvage two of the boats damaged on 2 August.[63]

The second of the two instances of Cold War 'shadow boxing' on which this chapter focuses for illustrative purposes also took place in 1964. In this instance, in contrast to the Tonkin Gulf Affair, a multiplicity of overlapping data shadows led the Johnson administration to an accurate conclusion: namely, prediction and ultimate detection of

[60] Hanyok, above n 50, 176, 200. See Edward Drea, *Gulf of Tonkin Incident: Reappraisal 40 Years Later* (6 December 2006) HISTORYNET <http://www.historynet.com/gulf-of-tonkin-incident-reappraisal-40-years-later.htm>) 175-230; Pat Paterson, 'The Truth About Tonkin' (2008) 22(1) *Naval History Magazine* < https://www.usni.org/magazines/navalhistory/2008-02/truth-about-tonkin>; John Prados, *Essay: 40th Anniversary of the Gulf of Tonkin Incident* (4 August 2004) National Security Archive <http://nsarchive.gwu.edu/NSAEBB/NSAEBB132/essay.htm>.
[61] Moïse, above n 5, 143 (describing doubts harboured by Captain John Herrick, commander of the Seventh Fleet's Destroyer Division 192 who was on board the *Maddox* and in charge of the mission).
[62] Hanyok, above n 50, 177.
[63] Hanyok, above n 50, 200-214. See Carl Otis Schuster, *Case Closed: The Gulf of Tonkin Incident* (8 July 2014) HISTORYNET <http://www.historynet.com/case-closed-the-gulf-of-tonkin-incident.htm>

the first detonation of an atomic bomb by the People's Republic of China on 16 October 1964.[64]

Early in 1964, US State Department officials were presented with Central Intelligence Agency (CIA) reports stating that Chinese officials had said that the final atomic test would 'definitely' occur in 1964.[65] Around these humint reports circulated a multi-source array of evidence. A September 1963 U-2 mission had returned photographs showing gaseous diffusion and thermal power plants at Lanzhou in northwest China.[66] In the spring of 1964, India agreed to the secret deployment of a U-2 detachment in Charbatia which allowed the US to obtain images of Lop Nur, some 1719 kilometres further to the northwest than Lanzhou (and also enabled India to gain access to the resulting intelligence).[67] A series of successful satellite reconnaissance missions conducted between mid-1963 and mid-1964 captured photographic imagery of China.[68]

[64] Jeffrey T Richelson, *Spying on the Bomb: American Nuclear Intelligence from Nazi Germany to Iran and North Korea* (WW Norton & Company, 2007) 167 (citing *Selections from* China Today*: National Defense S&T Undertakings*, (Joint Publications Research Service, JPRS-CST-94-009, 23 May 1994) 29; John W Lewis and Litai Xue, *China Builds the Bomb* (Stanford University Press, 1991) 187; Note, 'Nuclear Pursuits' (1991) 47(4) *Bulletin of the Atomic Scientists* 49).
[65] Richelson, *Spying on the Bomb* above n 64, 158.
[66] Richelson, *Spying on the Bomb* above n 64, 158 citing National Photographic Interpretation Center, *Mission GRC 176, September 25, 1963*, October 1963, 13-14, 17.
[67] Richelson, *Spying on the Bomb* above n 64, 158 (citing Chris Pocock, *Dragon Lady: The History of the U-2 Spyplane* (Airlife, 1989), 98; M S Kohli and Kenneth Conboy, *Spies in the Himalayas: Secret Missions and Perilous Climbs* (University Press of Kansas, 2003) 23-25; Interview with Richard Bissell (Farmington, Connecticut, 16 March 1984; 'Wheelon interview') [unable to verify full citation of interview]).
[68] Richelson, *Spying on the Bomb* above n 64, 159 (citing Dwayne A Day, John M Logsdon and Brian Latell (eds), *Eye in the Sky: The Story of the CORONA Spy Satellites* (Smithsonian Institute Press, 1998) 233, 238; Robert A McDonald, 'CORONA: Success for Space Reconnaissance, A Look into the Cold War and a Revolution for Intelligence', (1995) 60(6) *Photogrammetric Engineering and Remote Sensing* 716; Chairman James Q Reber, Committee on Overhead Reconnaissance, *Memorandum for: Director of Central Intelligence, Subject: Additional KH-4 Coverage of China* (17 April 1964) CREST NARA).

Lop Nur was photographed during several of these missions, in February and late April 1964; the April imagery revealed that a tower had been constructed at this site.[69]

This photographic evidence formed the basis of a report by CIA Director John A. McCone to President Johnson on 24 July 1964 that the U-2 spy-planes and reconnaissance satellites had observed five installations associated with the Chinese program 'in various stages of assembly and operation'. McCone advised, in summary: '[E]vidence on Communist China's nuclear weapons program is still insufficient to permit confident conclusions as to the likelihood of Chinese Communist detonation in the next few months … [but the CIA believed that] Communist China's leaders are determined to set off a nuclear device at the earliest possible moment in order to secure military, psychological, and political advantages'. [70]

In August 1964, analysts at the National Photographic Interpretation Center (a major producer of interpretations of satellite imagery throughout the Cold War) completed a study, largely based on aerial and satellite imagery, of Jiuquan in northwesternmost China. They noted: 'one possible reactor building completed, a large probable reactor building under construction, and a possible chemical separation plant'. [71] On 9 August 1964, a US reconnaissance satellite ejected film recovery capsules containing four

[69] Richelson, *Spying on the Bomb* above n 64, 159 (citing National Photographic Interpretation Center, NPIC/R-740/64; *Probable Atomic Energy Complex Under Construction near Chih-Chin-Hsia, China*, August 1964, 7, CREST, NARA; National Photographic Interpretation Center, NPIC/R-155/64, *Oak-Part I, Mission 1004-2, 19-22 February 1964*, February 1964, 17, CREST, NARA).
[70] Richelson, *Spying on the Bomb* above n 64, 159-60 (citing John McCone, Memorandum for the Record, July 24, 1964, in Harriet Dashiell Schwar (ed), *Foreign Relations of the United States, 1964-68, Volume XXX*, 70; CIA, "Communist Chinese Nuclear Weapons Capabilities", July 22, 1964.)
[71] Richelson, *Spying on the Bomb* above n 64, 160 (citing National Photographic Interpretation Center, NPIC/R-740/64, *Probable Atomic Energy Complex Under Construction near Chin-Chin Hsia, China*, 1-5). The NPIC was established by President Eisenhower at the very end of his term to analyse intelligence obtained from aerial and geospatial photography: Central Intelligence Agency, *A Look Back…The Founding of the NPIC, 1961* (20 June 2008) <https://www.cia.gov/news-information/featured-story-archive/2007-featured-story-archive/a-look-back-the-founding-of-npic-1961.html>.

days' worth of imagery of facilities at Jiuquan and at the Lop Nur site. CIA experts concluded on the basis of this data that Lop Nur 'is a nuclear test site which could be ready for use in about two months'.[72]

In the face of disagreement among US intelligence analysts about the soundness of this conclusion, CIA Director McCone sought and was ultimately granted presidential approval for a further U-2 overflight over the Lop Nur test site, but the U-2 mission in question was cancelled in the face of the impending US presidential election. [73] By late September, however, consensus appeared to have been reached among leading US intelligence analysts that preparations at the Lop Nur site were basically complete, the basis of which was largely, it seems, satellite photography.[74] On 15 October 1964, the head of the Office of Scientific Intelligence Donald Chamberlain is reported to have confirmed that recent information (most likely imagery obtained from US reconnaissance satellites in September and October of that year) indicated that Lop Nur was probably ready to host an atomic test.[75] The next day, on which China detonated its first atomic bomb at Lop Nur, eleven of the US Atomic Energy Detection System's thirteen electromagnetic pulse detection stations picked up indications of an atomic bomb test. Their data also produced the estimated time of the detonation and contributed to the initial yield estimate. Seven acoustic stations also detected signals

[72] Richelson, *Spying on the Bomb* above n 64, 160 (citing Frederic C E Oder, James C Fitzpatrick, Paul Worthman, *The CORONA Story* (National Reconnaissance Office, 1997) 155; Director of Central Intelligence, SNIE 13-4-64, *The Chances of an Imminent Communist Chinese Explosion*, August 26, 1964 in Kevin Ruffner (ed), *CORONA: America's First Satellite Program* (CIA, 1995) 239, 239). See also Jeffrey T Richelson, *The Wizards of Langley: Inside the CIA's Directorate of Science and Technology* (Basic Books, 2008).
[73] Richelson, *Spying on the Bomb* above n 64, 161-63.
[74] Ibid 165.
[75] Ibid.

indicating a test, which helped the US to estimate the yield and location of the detonation.[76]

In each of these two Cold War incidents, US perceptions of the actions and intentions of major Communist nations were refracted through a diffuse range of data points, technologies, and collection and analysis locales. Vital international legal decisions – judgments relevant to the implementation of *jus ad bello* (or the international law of armed conflict) and *jus in bellum* (or international humanitarian law), for instance – rested not so much on high-level human assessment of other humans, as on hybrid (human-nonhuman) accumulations and translations of piecemeal, scattered, electronic data. We may have come to understand these incidents as clashes between sovereigns, but they might just as easily be understood as dizzying dances among data shadows of a kind that, long after the Cold War, have come to seem ubiquitous on the global plane.

[76] Ibid 167 (citing Air Force Technical Applications Center, *History of the Air Force Technical Applications Center, 1 July – 31 December 1964*, n.d., 9, 11, 15; "Selections from CHINA TODAY: National Defense S&T Undertakings", *Joint Publications Research Service*, JPRS-CST-94-009, May 23, 1994, 30).

V Conclusion

Throughout the Cold War and in the first decade of its aftermath, international lawyers devoted considerable effort to trying to disabuse their discipline of the so-called 'billiard ball' model of legal and political affairs identified with the Cold War predominance of Realist thinking in international relations. That is a model premised on the determinative authority of sovereign states and their political leaders and an assumption that those leaders 'respond to reward and punishment contingencies specified by the structural balances of power and interests among the states in the international system'.[77] It also encouraged 'analysis in terms of government organs and of the technical doctrines employed by [high-level state] officials' rather than in terms of social norms, behavioural factors, or the quirks and uncertainties of actual practice.[78]

Critics of this approach argued for a more complex, multi-valent model of international order in which international law could be seen to play a vital, directive role at many sites and scales of interaction, and to be engaging a wide range of human actors.[79] What these critics may have underestimated, however, was the extent to which the appeal of the Realist model of global affairs, and its expression in 'conventional' international law, may have been less an expression of blind adherence to a 'myth system' and more a manifestation of, and reaction to, disorientation provoked by Cold War diffusion and multiplication of data in global affairs.[80]

In lieu of billiard balls, international lawyers have advanced a succession of 'comprehensive, analytic framework[s]' and 'conceptual technique[s] for mapping the relevant processes'. [81] However, they have done so, by and large, without taking

account of the extent to which international law was, over the course of the Cold War, 'unhomed' (that is, made *unheimlich* or uncanny) by the prevalence of data shadows.[82] Perhaps accurate, comprehensive maps of the world's complex workings and routes for their lawful navigation were not what many were looking to international law to provide, so much as a highly reductive framework for ranking and wrangling the profusion of data shadows crowding around them – a framework that might help those ostensibly in power, and those aspiring to power, to feel more at home in the world.

The techno-legal innovations of the Cold War ushered in an international legal order in which decision-making on legal issues often entailed engaging, and giving effect to, human-nonhuman approximations of action and intent on the part of states and other actors – approximations often rendered, in multiple, in electronic data. This imperative

[77] Stephen G Walker, 'Macropolitics and Foreign Policy Decisions: The Billiard Ball Model of IR', in Stephen G Walker, Akan Malici and Mark Schafer (eds), *Rethinking Foreign Policy Analysis: States, Leaders, and the Microfoundations of Behavioral International Relations* (Routledge, 2010) 21, 23.
[78] W Michael Reisman, Siegfried Wiessner and Andrew R Willard, 'The New Haven School: A Brief Introduction' (2007) 32 *Yale Journal of International Law* 575, 577.
[79] Influential among such critiques and counter-narratives put forward during the Cold War were those advanced by Myres McDougal and Harold Lasswell. See, e.g., Myres McDougal, 'International Law, Power and Policy: A Contemporary Conception' (1953) 82 *Collected Courses of The Hague Academy of International Law* 137; Myres McDougal, 'The Realist Theory in Pyrrhic Victory' (1955) 49 *American Journal of International Law* 376; Myres McDougal, 'Some Basic Theoretical Concepts about International Law: A Policy-Oriented Framework of Inquiry' (1960) 4 *Journal of Conflict Resolution* 337; Myres S McDougal, Harold D Lasswell and W Michael Reisman, 'The World Constitutive Process of Authoritative Decision' (1967) 19 *Journal of Legal Education* 253; Myres S McDougal, Harold D Lasswell and W Michael Reisman, Theories about International Law: Prologue to a Configurative Jurisprudence' (1968) 8 *Virginia Journal of International Law* 188. For retrospective analysis of their project near the Cold War's end, see Gray L Dorsey, 'The McDougal-Lasswell Proposal to Build a World Public Order' (1988) 82 *American Journal of International Law* 41. A key figure in the 1990s version of this effort was Anne-Marie Slaughter (also known as Anne-Marie Burley). See, e.g., Anne-Marie Slaughter Burley, 'International Law and International Relations Theory: A Dual Agenda' (1993) 87 *American Journal of International Law* 205; Anne-Marie Slaughter, 'International Law in a World of Liberal States' (1995) 6 *European Journal of International Law* 503.
[80] The term 'myth system' and the idea of 'conventional' international law as embedded with Realist precepts are taken from: Reisman, Wiessner and Willard, above n 78, 577.
[81] Ibid.
[82] I am drawing here, with considerable imprecision, from Freud's notion of the uncanny which (borrowing from Friedrich Schelling) Freud defined as 'the name for everything that ought to have remained secret and hidden but has come to light', and for the sense of strangeness that one may experience when impressions of such hidden things are evoked: Sigmund Freud, 'The "Uncanny"' in James Strachey (ed), *The Standard Edition of the Complete Psychological Works of Sigmund Freud, XVII*, (Hogarth Press, 1971) 217, 224.

emerged notwithstanding (and operated alongside) the persistence of formal, doctrinal preoccupations with ensuring definitive attribution to, and explicit consent from, states in order for them to be legally bound, as if matters of state conduct and will were relatively straightforward to resolve, in exclusively human-to-human ways.[83]

Cold War international law thus remained formally embedded with expectations of rational clarity and control on the part of highly ranked humans, while being increasingly stalked by, and answerable to, shifting, multiplying apparitions in data that routinely confounded those expectations. In this sense, the experience of their Cold War counterparts may afford contemporary international lawyers – grappling with 'post-truth politics', the proliferation of 'alternative facts' and a deluge of data in unmanageable dimensions and a dizzying diversity of forms – an example of earlier iterations of more or less comparable struggles.[84]

[83] See *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits)* [1986] ICJ Rep 14 regarding the definitive attribution requirement for state responsibility. See also *Vienna Convention on the Law of Treaties*, opened for signature 23 May 1969, 1155 UNTS 331 (entered into force 27 January 1980) regarding the requirement that state parties make their consent explicit (by signature or ratification) in order to be bound.
[84] Fleur Johns, 'The Deluge' (2013) 1 *London Review of International Law* 9. On 'post-truth politics' and 'alternative facts', see Jim Rutenberg, 'The Costs of Trump's Brand of Reality', *The New York Times* (New York), 23 January 2017, B1. For scholarly analysis of this phenomenon with regard to the US, the UK and Europe, see Oscar David Barrera Rodriguez et al., 'Facts, Alternative Facts, and Fact Checking in Times of Post-Truth Politics' (2017) <https://ssrn.com/abstract=3004631>.