Leaks:
Secure Communications and
Achieving Nuclear Zero

Bruce D. Larkin

Dismantling and prohibiting nuclear weapons, and then maintaining a stable peace in a non-nuclear world, will require ongoing political negotiations and collaborative actions, which some will seek to undermine, distort, preclude, or simply shape in hope of outcomes judged more in their interest. This is the nature of politics and life in a social world. Negotiation is the distinguishing activity of politics. It is carried on among ‘friends’, among those in search of the like-minded, and between ‘enemies’. It is carried on within governments, and between ‘parties’ and their publics.

Secure communication serves not only the actual negotiation, exchanges between negotiators, but other purposes as well: intelligence (gathering ‘facts’ about the world), coordination (for example, among officials of a government), and operations (covert and military). It is widely held that governments are advantaged if others do not know the sources, content and quality of intelligence available to them, their internal arguments, and their action plans, both strategic and tactical. To preserve these perceived advantages governments endeavor, by many means (recruitment, training, document control, sanctions, and denial of access, as well as control of communications), to define ‘secrets’ or ‘military secrets’ or ‘state secrets’ and then prevent their unauthorized ‘leakage’.

This paper explores the role of ‘secrecy’ and its breach, with
focus on efforts to achieve and sustain ‘zero nuclear weapons’ (ZNW).

Secure Communications and Nuclear Weapon ‘Management’

In a 2006 paper I posed this question: “If Washington could get so much wrong in invading Iraq, can we be confident of its management of nuclear weapons?” I concluded that

we cannot be confident of the current management of US nuclear weapons. The better posture is one of scepticism toward claims that any system of command and control can meet the standards of coherence, robustness, reliability and performance which ongoing ‘nuclear weapons management’ requires.

About sources of possible breakdown I cited “assumptions about the loyalties and performance of their personnel” and comment by a naval information systems manager that another ‘Johnny Walker’ can’t be ruled out.

Through history people have intentionally or unintentionally passed classified information. There are people like Johnny Walker around. We’ve had them in the past; we’ve had them recently. We’ll have them again. But, the vast majority of our military people have the personal integrity and the training that keeps them from violating security rules.

Of course successfully reading information on a secure network


2 Ibid., p. 114.

does not imply an ability to disrupt the communications it carries, plant false information, or falsify commands (‘spoof’).

This paper centers not on military operations, such as command and control of nuclear weapons, but on (i) the relationship between secure communication and the politics of achieving global zero and (ii) what experience suggests about the consequences of security breaches.

**The Zimmermann Telegram**

Internal communications of governments are susceptible to interception. A classic case is that of the Zimmermann Telegram, an instruction from the German foreign minister to the German ambassador in Mexico City, during WWI. In brief, he was told to inform the government of Mexico that if it joined war between Germany and the United States its reward upon victory would be a large part of the southwestern United States.4

Britain was routinely intercepting and decoding cable traffic passing through the Caribbean. The United States had not joined the war against the Central Powers, but under the presidency of Woodrow Wilson had held itself out. Revelation of Germany’s approach to Mexico, however, catalyzed a US decision to join with Britain and France, and may have decisively altered the outcome of the war.

**The Pentagon Papers**

The US Secretary of Defense during the Vietnam War directed that there should be assembled a record of key decisions, drawing on the archive of communications. A group was assigned the task, and

---

performed it even as the war dragged on.5

One participant in the process, Daniel Ellsberg, concluded that the record should be made public and thereupon ‘leaked’ the text to The New York Times. On 13 June 1971 the Times began publication of a series of articles based on the material. In July it published a selection of the papers, with commentary, in a single volume.6 Times reporter Neil Sheehan wrote that

Though far from a complete history, despite their bulk, the Pentagon papers form a great archive of government decision-making on Indochina over three decades. The papers tell what decisions were made, how and why they were made and who made them. The story is told in the written words of the principal actors themselves—in their memorandums, their cablegrams and their orders—and in narrative-analyses of these documents written by the 36 authors of the history.7

Reconstructed Cables From the Teheran Embassy Seizure

When Iranian militants overran the US Embassy in Teheran in November 1979 they not only seized hostages but also gathered the material remains of a large number of diplomatic and intelligence cables. Embassy staff had endeavored to destroy these by shredding, using a machine that turns sheets of paper into long narrow strips of confetti. But with enormous patience—and perhaps helped by the proximity of strips from the same document in shredder output as bagged—the militants reconstructed the cables. They then issued copies of the cables in a face-to-face (or side-by-side) edition in English and Persian running some 70 ‘volumes’ or bound slips given the title “Documents From the U.S. Espionage Den.”

The time was the early 1980s, when it was not possible to find these cables on the Net, nor could people in the United States order

---

5 According to The New York Times, the top-secret history combined 3000 pages of narrative with 4000 pages of appended documents, totaling 47 volumes.
7 Ibid., p. x. 2 July 1971.
them from Amazon. The (private) National Security Archive issued some as a ‘document collection’, and describes how the cables first came into the United States and became the subject of an article in the *Washington Post*:

The genesis of this document collection was the reporting done by Scott Armstrong for his five-part series entitled “The Fall of the Shah,” published in the *Washington Post* from October 25-30, 1980. This series revealed the existence of a major internal Carter administration review of U.S.-Iranian relations, the so-called “White Paper” process discussed below. Armed with this revelation, Max Holland, then at the American Friends Service Committee, and several other researchers filed Freedom of Information Act requests for the White Paper itself and for the background documents used in its preparation. Over a period of more than six years, the documents trickled in as the result of a continuing appeal and negotiation process with the State Department. Holland graciously donated his collection of these materials to the National Security Archive; combined with Armstrong's materials, they represent a significant portion of the published set.

The “Documents from the U.S. Espionage Den” were first brought to the United States from Iran by freelance journalists William Worthy and Randy Goodman in December 1981. The 13-volume set they attempted to bring in with their luggage was confiscated by the U.S. Customs Service; however, a second set which they sent through the mail arrived safely. Worthy and Goodman brought the volumes to Scott Armstrong’s attention. The subsequent five-part series of *Washington Post* articles titled “Iran Documents Give Rare Glimpse of a CIA Enterprise,” beginning on January 31, 1982, brought these documents to national attention.8

---

8.  The National Security Archive is online at http://www.nsarchive.org . Its original publication of the Teheran embassy trove was on microfiche. The text quoted here, describing acquisition of the cables, is online at http://elmgostar.ir/PRODUCT/digital/digital%202/IranIran%20The%20Making%20of%20U.S.%20Policy.htm . The Archive, in EBB No. 21 [below], wrote this of the microfiche and its project on Iran:

One of the Archive’s first major microfiche publications, *Iran: The Making of U.S. Policy, 1977-1980* (Alexandria, VA: Chadwyck-Healey, 1990) reproduced some 14,000 pages of declassified materials, including many documents seized and later published by the “Students Following the Line of the Imam” who overran the U.S. embassy in November 1979. The U.S.-Iran Project is also seeking new materials from British and former Soviet archives, given the crucial impact of those countries’ policies on Iran during the Cold War.

The undated presentation at elmgostar.ir includes this Archive explanation:

---

The genesis of this document collection was the reporting done by Scott Armstrong for his five-part series entitled “The Fall of the Shah,” published in the *Washington Post* from October 25-30, 1980. This series revealed the

---

Bruce D. Larkin. *Leaks: Secure Communications and Achieving Nuclear Zero*
The 72 volumes are accessible online via a page at the Internet Archive, an organization unrelated to the National Security Archive. The Internet Archive endeavors to maintain a cumulative record of material of cultural significance appearing on the Net and Web. An example of the cables available is reproduced below. Compare the quality, however, of a cable reconstituted from shreds. However difficult it may be to read the reconstituted cables, they are more than sufficient to identify a text that could be sought in other sources, if published, or as the object of a Freedom of Information Act request.

existence of a major internal Carter administration review of U.S.-Iranian relations, the so-called “White Paper” process discussed below. Armed with this revelation, Max Holland, then at the American Friends Service Committee, and several other researchers filed Freedom of Information Act requests for the White Paper itself and for the background documents used in its preparation. Over a period of more than six years, the documents trickled in as the result of a continuing appeal and negotiation process with the State Department. Holland graciously donated his collection of these materials to the National Security Archive; combined with Armstrong's materials, they represent a significant portion of the published set.


10. [Cable example:] File v30_text.pdf, p. 102. Cable KABUL 7252. 1 October 1979. [Reconstituted cable example:] File v30_test.pdf, p. 140. Cable identification and date (except October 1979) indistinct.
Bruce D. Larkin.  Leaks: Secure Communications and Achieving Nuclear Zero
‘How Hacker Penetrated the Heart of British Intelligence’

According to newspaper accounts, a ‘hacker’ gained access to the addresses and telephone numbers of a broad array of British intelligence facilities. In fact it was no ‘hacker’ at all, but a
temporary BT employee who exploited the fact that sensitive passwords were posted prominently for the convenience of staff. One account has it that

Telephone numbers and addresses for MI6, MI5 many secret Ministry of Defense installations and other very sensitive information were copied from the [BT] computer ...[as well as] home addresses of senior military personnel; details of phone installations for the secret US communications station at Menwith Hill in North Yorkshire; information about the bunker in Wiltshire where the Government would go in the event of a nuclear war; and telephone installations in Downing Street and Buckingham Palace.  

This case illustrates vulnerability to a ‘trusted insider,’ especially when the ‘insider’ has sought work with mischief in mind. The Independent, it reported,

has been able to verify the authenticity of the information which runs to hundreds of thousands of words and numbers and appears as internal BT records taken straight off the computer.

A GCHQ Employee Releases a US National Security Agency Memorandum Tasking Those Conducting Surveillance on UN Delegations

In the jostling prior to GW Bush attacking Iraq on 19 March 2003 the United States sought to win UN Security Council approval of an attack. What was sought was a 'second resolution’. It was thought that the United Kingdom would not join in war against Iraq unless a ‘second resolution’ was obtained, but in the event that proved not

---


12 For several (unattributed) texts about this exploit, including one by the employee, Steve Fleming, himself, see http://securitydigest.org/risks/mirror/ftp.sri.com- risks/16/risks-16.58bt Fleming contended he merely wished to show that it was possible, after which he informed the authorities.

13 Kelsey, above.

Bruce D. Larkin. Leaks: Secure Communications and Achieving Nuclear Zero
the case.

The US version of ‘necessity’ turned on imminent threat from Iraqi ‘weapons of mass destruction’, and especially nuclear weapons. At stake was whether the IAEA and UNMOVIC inspections in Iraq should run their course, exhausting the question whether there was evidence that Iraq was moving to acquire ‘weapons of mass destruction’, or whether the inspections should be shoved aside unless they produced the evidence sought. In this sense the pre-war political maneuvering of 2002 and early 2003 was homologous with what could be expected of suspicions or charges of ‘breakout’ from a ZNW world.

While the United States still thought that it might obtain approval by the P5 and sufficient members of the Security Council, a National Security Agency staff member sent an email to staff in New York directing acquisition of intelligence about the intentions of states that were members of the Security Council.\textsuperscript{14} A copy of this message was (routinely, we presume) forwarded to the NSA’s counterpart in the UK, GCHQ. Katherine Gun, a translator employed at GCHQ, made the text public. She was subsequently placed on trial, but the process was abandoned in midcourse, and she was released.\textsuperscript{15}

Comment at the time raised the question how the intimate relationship between NSA and GCHQ could be maintained if NSA doubted the British Government’s ability to ensure that shared secret US documents were not leaked.

This is the text of Koza’s message:\textsuperscript{16}

\textsuperscript{14} Cf. James Banford, \textit{The Shadow Factory}, p. 142.


To: [Recipients withheld]
From: FRANK KOZA, Def Chief of Staff (Regional Targets) CIV/NSA
Sent on Jan 31 2003 0:16
Subject: Reflections of Iraq Debate/Votes at UN-RT Actions + Potential for Related Contributions
Importance: HIGH
Top Secret//COMINT//X1

All,

As you've likely heard by now, the Agency is mounting a surge particularly directed at the UN Security Council (UNSC) members (minus US and GBR of course) for insights as to how to membership is reacting to the on-going debate RE: Iraq, plans to vote on any related resolutions, what related policies/ negotiating positions they may be considering, alliances/ dependencies, etc - the whole gamut of information that could give US policymakers an edge in obtaining results favorable to US goals or to head off surprises. In RT, that means a QRC surge effort to revive/ create efforts against UNSC members Angola, Cameroon, Chile, Bulgaria and Guinea, as well as extra focus on Pakistan UN matters.

We've also asked ALL RT topi's to emphasize and make sure they pay attention to existing non-UNSC member UN-related and domestic comms for anything useful related to the UNSC deliberations/ debates/ votes. We have a lot of special UN-related diplomatic coverage (various UN delegations) from countries not sitting on the UNSC right now that could contribute related perspectives/ insights/ whatever. We recognize that we can't afford to ignore this possible source.

We'd appreciate your support in getting the word to your analysts who might have similar, more in-direct access to valuable information from

"Online document: The text of the memorandum detailing the US plan to bug the phones and emails of key Security Council members, revealed in today's Observer."

accesses in your product lines. I suspect that you'll be hearing more along these lines in formal channels - especially as this effort will probably peak (at least for this specific focus) in the middle of next week, following the SecState's presentation to the UNSC.

Thanks for your help.

**Wikileaks**

By comparison to the leak of Frank Koza’s single email, the release through Wikileaks of numerous US military communications concerning the wars in Iraq and Afghanistan and then, monumentally, 251,287 US State Department instances of ‘cable traffic’ seems to suggest that the very notion of ‘secure communications’ is in doubt. Should we conclude from the Wikileaks ‘cablegate’ release that there is no longer any possibility of ‘secure communications’, and therefore no place for an expectation that ‘secure communications’ will play a part in the political process leading to denuclearization?

Consider these observations about the ‘cablegate’ messages:

- None we have seen are classified higher than ‘secret’, and some are merely ‘confidential’. No ‘top secret’ messages have been shown, nor any designated ‘special compartmented information’ (SCI).\(^\text{17}\)

- Among those classified ‘confidential’ are reports of conversations with foreign officials who, unsurprisingly, already knew what had been said.

- Some cables that document embarrassing US initiatives—such as those calling for collection of personal biographic

---

information about foreign officials—simply confirm what has long been believed.

- Most of the cables we have seen simply confirm US policy initiatives and postures which are simple expressions of US interests, reveal no skulduggery, and could have been said in public. (In fact, some are simply ‘talking points’ designed to ensure that what is said in public by diplomats in US embassies conforms to US policy.)

In the spirit of ‘the exception that proves the rule’, however, consider a cable regarding a complex issue expected to come before the 2010 NPT Review Conference: calls for creating a nuclear-free zone in the Middle East, with implications for Israeli nuclear weapons. The US reveals a design to outflank the Egyptian Foreign Minister by going directly to President Mubarak. Consider this excerpt from a cable sent on 20 February 2010:

SECRET SECTION 01 OF 03 PARIS 000193

NOFORN
SIPDIS

E.O. 12958: DECL: 02/19/2020
TAGS: PREL PARM MNUC KACT KNNP MARR MCAP NATO CH IR, PK, FR
SUBJECT: U/S TAUSCHER’S MEETINGS WITH FRENCH OFFICIALS

Classified By: DCM Mark Pekala, Reasons 1.4 (b), (d).

¶1. (C/NF) SUMMARY: Under Secretary of State for Arms Control and International Security Ellen Tauscher’s February 2 meetings with French counterparts from the Elysee (presidency) and MFA included discussions of U.S. disarmament priorities, the NPT Review Conference (NPT RevCon), the Nuclear Security Summit, and missile defense. Meeting separately with NSA-equivalent Jean-David Levette, Presidency Strategic Affairs Advisor Francois Richier, and MFA Strategic Affairs Director Patrick Maisonnave, U/S Tauscher reassured the French that while “a world without nuclear weapons” is a sincere USG ambition, the

Bruce D. Larkin. Leaks: Secure Communications and Achieving Nuclear Zero
United States will not move precipitously and will take allies’ interests into account. U/S Tauscher discussed next steps on NPT RevCon preparations, including thinking creatively about outcomes and minimizing the threat of disruptive Egyptian behavior. U/S Tauscher also clarified USG missile defense priorities, especially political support for territorial defense at the 2010 Lisbon NATO summit. END SUMMARY.

¶6. (S/NF) Richier and Maisonnave agreed with U/S Tauscher’s analysis that Egyptian FM Aboul-Gheit will, if unchecked, work to undermine the RevCon with an aggressive posture on the Middle East Nuclear Weapons Free Zone (NWFZ) resolution. U/S Tauscher outlined ongoing U.S. efforts to gain consensus language on the NWFZ, but underlined the need to contemplate a more forward-leaning strategy. She suggested considering possible phone calls from Presidents Obama and Sarkozy directly to Egyptian President Mubarak in the mid-March timeframe to sensitize the Egyptian president to the importance of the RevCon in strengthening the NPT and the unhelpful role the Egyptian MFA is playing.18

This message illustrates several problems. While the French participants in conversations with Ellen Tauscher knew the contents of their talks, other governments—including the Egyptian government—probably did not. US officials had concluded that the likelihood of influencing Egypt’s position would be enhanced if both Obama and Sarkozy approached Mubarak by telephone; hence the effort to concert US and French action. Mubarak might suspect that Washington and Paris had exchanged preliminaries about the telephone approach, but would not have had evidence to that effect.

From this cable alone it isn’t possible to discern what other steps the United States may have been taking to achieve a Middle East resolution to its liking. We do know that at the NPT Review Conference language was reached that no participant rejected, after difficult negotiations, and that the result was credited in part to the role taken by Ireland’s Alison Kelly.

18 Cable 10PARIS193. NOFORN or NF means ‘no foreign dissemination’. [Arkin translates it as ‘Not Releasable to Foreign Nationals’.] SIPDIS indicates the message is suitable for dissemination on SIPRNET, the ‘Secret Internet Protocol Router Network’, an internal US government network.
The ‘cablegate’ messages contribute nothing to an understanding how a government or private entity could ‘hack’ a government’s secure communications. Instead, ‘cablegate’ confirms the well-understood fact that terming communications ‘secure’ accepts a risk that some person authorized to access the system will divert or alter its contents. That is what reporters’ accounts of the episode have claimed: that a US Army private, with authorized access and a ‘Top Secret/SCI’ clearance, devised a subterfuge to copy and remove the texts of the cables from a ‘secure’ facility in Baghdad. 19

The result is that (as of 2 January 2011) about 2000 cables had been widely distributed on the Net, and some of them summarized and even reproduced in full (or with some selective redactions) by Der Spiegel, El Pais, Le Monde, the Guardian, and the New York Times. By the end of 2010 it was also reported that the full set had been placed in the hands of Aftenposten and Novaya Gazeta.

The US Government confronts the anomaly that texts marked ‘Secret’ and ‘NOFORN’ are nonetheless loose in the wild and cannot be recalled. And the New York Times reports that

The [US] Air Force is barring its personnel from using work computers to view the Web sites of The New York Times and more than 25 other news organizations and blogs that have posted secret cables obtained by

19 See “Military Bans Removable Media After WikiLeaks,” CBS News, 10 December 2010. http://www.cbsnews.com/stories/2010/12/10/tech/main7138053.shtml; and Robert Booth, Heather Brooke and Steven Morris, “WikiLeaks cables: Bradley Manning faces 52 years in jail,” The Guardian, 30 November 2010. “Manning faces a court martial and up to 52 years in prison for his alleged role in copying the diplomatic cables, as well as the leak of military logs about incidents in Afghanistan and Iraq and a classified military video which showed a crew of an American Apache helicopter gunning down a group of men who they thought had a rocket launcher. They turned out to include Reuters staff with a TV camera.”
WikiLeak, Air Force officials said …

Do those holding US security clearances jeopardize themselves if they read, or share, texts that are accessible to a billion other people? This must not be a silly question, since Jeffrey Lewis has addressed it on his armscontrolwonk.com blog, in the following way:

I know that a lot of my readers have .gov and .mil addresses, which means that I need to take special care about how I treat classified material on this website.

I’ve spent a few days talking to people, and there are no easy answers. Each element of the government seems to have its own policies, which are evolving over time.

Until further notice, I am adopting the following policy when it comes to treating classified material, particularly that released by Wikileaks. (I have updated previous posts to conform with this policy.)

1. Under no circumstance will I post quotations that include security markings. I may quote from documents, but I won’t put anyone in the position of having a scarlet S or the dreaded NOFORN appear on their screen and, as a result, in their cache.

2. Under no circumstance will I post either the full-text of a cable or even consecutive paragraphs. In fact, I doubt that I will ever post the entirety of a paragraph. Any material taken from the cables will appear as it might in the New York Times or Washington Post.

3. I will do my best to enforce this policy on reader comments.

I hope that this satisfies the majority of readers with day jobs. In any event, I invite readers to comment on the new policy and am prepared to modify it if and when circumstances dictate.

---


21 Jeffrey Lewis, armscontrolwonk.com, 9 December 2010. A germane comment was posted by ‘anon’, in response to critics:

You do not understand the problem that Jeffrey is trying to solve. First, someone who works for the government, in general, and holds security clearances, in
The question whether Americans who read Wikileaks cables may be punished for doing so remained an issue, even more than two months after the cables began to appear on the Web. It was a bridge too far when the US Air Force threatened *family members* of personnel holding security clearances, if the family member read a classified cable.22

How is the currency of the ‘cablegate’ disclosures relevant to secure communication on the road to nuclear zero?

*Secrecy in Nuclear Weapon Doubt and Verification*

‘Secure communications’ do not matter if the content of those communications is sharable from the start. It is one thing if classification is the *default option*, declassification requiring that some burden of proof be met, and quite a different matter if non-classification is the default option, against which whomever proposes that the communication be classified must meet some serious demonstration of need and appropriateness.

---

22. Guardian, 8 February 2011. “US Air Force backtracks over WikiLeaks ban.” The report states: “The US air force has backtracked after issuing guidance last week banning the families of staff from reading classified material released by WikiLeaks. The guidance also warned that the families faced prosecution as spies if they read the leaked diplomatic cables. But the air force, seeking to calm a growing row, said on Monday night that the advice had not been sanctioned by headquarters and it had been removed from its website.” http://www.guardian.co.uk/world/2011/feb/08/us-air-force-wikileaks-families-banned-classified-material
By clearly distinguishing transactions and texts that require being private from those that do not, and following a policy of full disclosure wherever the requirement of privacy or secrecy cannot be persuasively made out, an institution confines its ‘secrets’ to the smallest number. A firm that designs, manufactures, and sells precision equipment probably has many ‘proprietary secrets’ that are the basis of its business. But if it finds there is some fault that could harm users or produce anomalous results it must share that fact with the buyers. Organizations also identify ‘personnel’ files as private, sometimes for the improper purpose of avoiding litigation, and sometimes with the understanding that papers may be released only with the consent of the employee. The case for secrecy can only be made around particulars.

In the transition to nuclear zero nuclear weapon states may claim that as the number of weapons declines their vulnerability increases, with the result that some facts become even more closely held than before. The N5 can tell the world how many nuclear weapons they have, but they will more jealously guard the locations of at least some of those weapons, an argument for the ‘jump to zero’ from several hundred.

Similarly, if the issue is whether nuclear weapon states have declared all nuclear weapons and fissile material in their possession, there need be nothing ‘secret’ about the evidence they advance in showing that this is so. A state or authority that suspects error, or misrepresentation, in a state’s declarations may appropriately keep its reasons to itself, for example treat an informant’s identity as a ‘secret’, but it must collaborate in the design of tests that will confirm or disconfirm its suspicions in circumstances free of secrecy. The same test applies mutatis mutandis to other issues of doubt and verification.

Secrecy as a ‘Wasting Asset’

There is another reason why ‘secrets’ typically matter less than their
aura suggests. It is a commonplace among those discussing secrecy to point out that it is a ‘wasting asset’. A secret may be, and often is, temporary, on its way to becoming a non-secret. Except for something known only to a single individual, there is cost and inconvenience to translating a ‘known’ into a ‘secret’. And if the translation includes procedures to ‘protect’ the secret, such as encrypting it, the cost and inconvenience will grow as more vexing protections are put in place. British Telecom’s posting passwords in plain sight responded to the inconvenience of introducing newcomers to the passwords they needed to do their work.

That ministries of external affairs are ready to reveal their communications after 30 or 50 years demonstrates that diplomatic cables should carry a ‘tell-by’ date. Looking back at the header to 10PARIS193 we see that it is already equipped with a tell-by date: DECL: 02/19/2020. The relevant US State Department manual instructs that

> When possible, the classifier should choose a specific date or event within 10 years for declassification. When this is not feasible, information should be classified for 10 years unless that does not provide adequate protection, in which case the information may be classified for up to 25 years from date of origin. With the sole important exception outlined in b) below, information may not be classified for longer than 25 years at the time of its original classification. For telegrams, enter the duration markings/declassification instructions on the E.O. 12958 line.

which is exactly where the expression DECL: 02/10/2020 appears. The exception at ‘b)’ is for “information that would reveal the identity of confidential human sources or human intelligence sources.” But in the case of 10PARIS193 the sources are neither ‘confidential’ nor ‘intelligence’ sources. Note, however, that the language does not preclude a later decision to change the original declassification date.

---


Bruce D. Larkin. Leaks: Secure Communications and Achieving Nuclear Zero
This excursion into the Department of State’s handbook illustrates that the governing Executive Order anticipates that much ‘secret’ information will become stale and in just a few years no longer require secrecy.  

What Secrets are ‘Necessary’, or ‘Useful’, in Seeking and Then Sustaining Nuclear Zero?  

Distinguish, at the outset, national requirements from requirements of the nuclear zero regime.  

Governments committed to nuclear abolition—having decided to work for and achieve a global abolition regime, or having inherited as state policy the decisions of earlier governments—are not in a static situation, but must repeatedly reassure themselves, and answer any doubts among their people, that the regime remains real and sustainable. From this follow these desiderata:  

[1] means to monitor the regime, relying heavily on national means and cooperation with others, and including measures to detect any conspiracy or clandestine program that aims to breach the regime;  

[2] results of monitoring, whether technical (e.g. sensor data, satellite photographs) or collaborative (e.g. contributions from other governments);  

[3] successive internal assessments of the regime, given the facts as they are understood, and given that there may be significant disagreement about the quality and meaning of ‘facts’ available;  

[4] contingency plans (which would include how regime

24 On the content of Executive Order 12598, see http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html
institutions are to be approached and their capabilities invoked) to be drawn upon should the regime be broken in some respect that could endanger the safety or security of its population.

Each of these requirements depends, to some extent, on its not being known to any party, whether a state or some non-state entity, that has resolved to seek advantage (which might include extraordinary precautions in case of breach by another!) by breaching the regime, or creating prerequisites for a prompt breaching of the regime. The seeming paradox is that each state’s assuring itself that the regime is sound will necessitate its undertaking planning and collaborations that it will be unwilling to share with all … with the resulting possibility that others may suspect it of harboring designs to breach the regime … and that such suspicions cannot be completely resolved by the available measures of reassurance.

Regime institutions will have analogous requirements, as we know from our familiarity with the work of IAEA, or of UNSCOM/UNMOVIC and IAEA in Iraq. If the Authority were called upon to assess whether a State Party had created unpermitted technical capabilities that could be called upon to effect a prompt breach of the regime, it would need to assess whether it was being given the access required to make that assessment, or was instead in the ‘cat and mouse’ situation to which Hans Blix frequently referred. There would have to be communications between inspectors and the Authority. If technical monitors were installed their data would need to be communicated with integrity to the Authority.

Secure communication is not an incidental feature of a zero regime, nor something introduced mischievously, but lies at the very heart of the regime’s raison d’etre. The entire process of negotiating and committing to an abolition regime arises out of peril and distrust. If the weapons were not so destructive ‘abolition’
might be desirable but not necessary, and if all governments (and groups) could be trusted then formal commitments and regime institutions would be completely unnecessary.

If Detection of Conspiracies and Clandestine Programs is Among the Tasks for a Nuclear Zero Regime, Must It Also Anticipate the Secrecy and ‘Secure Communications’ of Plotters?

This would seem to put global zero regime institutions—alongside governments committed to the regime—into practicing something akin to ‘cyberwar’.

Several implications follow. The regime and ‘conspirators’ will design and use encryption and decryption techniques. Conspirators may exploit, and the regime seek to detect, messages hidden in otherwise open transactions (recalling messages to the resistance in WWII: “The crow will fly at dawn.”). Altogether novel means of communication will be sought (recall Herodotus’ story of the courier with a message tattooed on his scalp, then hidden by growing hair). Conspirators’ obtaining intelligence of the regime’s capabilities to detect will be among their highest priorities.

Just how global regime institutions should modulate their transactions with and reliance on the states’ intelligence capabilities, and the offerings of oppositionists and defectors, were well-developed themes in the work of UNSCOM/UNMOVIC and the IAEA in Iraq. Hans Blix refers obliquely to the claim that the United States distorted UN-accepted offers of communications assistance within Iraq to install sensors working for its own anti-Sadaam agenda. No general a priori guidance can be given, since the disposition to avoid becoming entangled in member state intrigues and purposes may be outweighed, given circumstances and the threat, by the specifics of any actual endangerment to the
regime.

If a Nuclear Zero Regime Requires ‘Secure Communications’, Can That Requirement Be Met?

The answer is simple enough: although there is always a risk that important secrets will be lost, or data ‘spoofed’, there is a well-practiced repertoire of means to achieve greater assurance and hedge against risk: encryption, redundancy, monitoring and, above all, ensuring that no key decision is so hurried that common sense and further inquiry cannot be brought to bear on the situation at hand.

I have elsewhere summarized the tensions between efficacy and secrecy in these terms:

Best practice is to conduct study, design, and discussion with others in the open. There third parties can see the reasons advanced, and judge them. A broader consensus can be built around attractive steps.

State planning groups, engaged in intense internal negotiations as well as contacts with their counterparts in other States, may need to keep ‘secrets’, at least for a time. After all, they must explore the grounds for agreement and bring agreement to completion. But those claiming need for ‘secrets’ bear the burden of proof.
Abbreviations

BT [A local British telephone company]
CBW Chemical and Biological Warfare
FMCT Fissile Material Control Treaty or Fissile Material Cutoff Treaty
GCHQ [UK] Government Communications Headquarters
IAEA International Atomic Energy Agency
ISODARCO International School on Disarmament and Research on Conflicts. Italian Pugwash Group.
MI5 [UK] Security Service
MI6 [UK] Secret Intelligence Service
NF, NOFORD No foreign dissemination
NPR Nuclear Posture Review
NPT Non-Proliferation Treaty [Treaty on the Non-Proliferation of Nuclear Weapons]
NSA [US] National Security Agency
UN United Nations
UNMOVIC United Nations Monitoring, Verification, and Inspection Commission
UNSC United Nations Security Council
UNSCOM United Nations Special Commission
WMD Weapons of Mass Destruction
ZNW Zero Nuclear Weapons

Revision History

2011.02.10 First published to web, with additions from initial draft of 2011.01.09.
2011.02.18 Typographical errors corrected.
The *Journal of Denuclearization Design* is a cumulative digital-only journal edited and issued by the Global Collaborative on Denuclearization Design.

Access to the *Journal* is at the GC.DD website: www.gcdd.net. Please direct correspondence and submissions to editor@gcdd.net.

Some rights reserved: this work, its contents pages, or any complete article or set of articles, may be distributed freely subject to the attribution, non-commercial, and no derivative works conditions of the Creative Commons license 3.0. ‘Attribution’ is met by including this page as the last page of the article.

Bruce D. Larkin is Professor Emeritus of Politics at the University of California at Santa Cruz, and the Convenor and Director of Studies of the Global Collaborative on Denuclearization Design. He is the author of *Nuclear Designs: Great Britain, France, & China in the Global Governance of Nuclear Arms* (1996); *War Stories* (2001); and *Designing Denuclearization: An Interpretive Encyclopedia* (2008).