Developing the International Law Framework to Better Address Cyber Threats: Role of Non-Binding Instruments

J. Herbach[1]

[1]Centre for Conflict and Security Law, University of Amsterdam

E-mail contact of main author: j.d.herbach@uva.nl

Abstract. Although certain cyber threats are addressed by more general international legal frameworks (for instance, the Convention on Cybercrime or the law of armed conflict), the distinctive risks involved with potential nuclear-related cyber-attacks argue in favor of addressing this threat through the legal framework dedicated to nuclear security. The international legal framework for nuclear security is comprised of two basic categories of international instruments – legally binding and legally non-binding. The primary treaties for nuclear security are the Convention on the Physical Protection of Nuclear Material (CPPNM), and its 2005 Amendment, and the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT). These treaties, however, are of limited application when it comes to addressing cyber threats, namely applicable with respect to specific criminalization provisions. However, modifying existing treaties or adopting new legally binding instruments in order to deal with evolving threats is a time-consuming process that may not be desirable or realizable, considering the difficulties in obtaining sufficient ratifications or accessions for entry into force of the CPPNM Amendment. Focusing on non-binding instruments (i.e. the Nuclear Security Series documents), on the other hand, offers distinct advantages. Non-binding instruments provide flexibility. They can be adopted more rapidly and amended or replaced relatively quickly if they do not meet current needs. They can also provide substantially more technical detail. In other words, emergent and still developing issues such as cyber threats lend themselves, perhaps better, to coverage under non-binding instruments. Considering the need to develop the international legal framework for nuclear security to better address cyber threats distinct to the nuclear field, the Nuclear Security Series recommendation-level documents, such as NSS 13, would be a good place to start.

1. Introduction

In devising the methods for addressing cyber threats to nuclear and other radioactive material and related facilities, it is necessary to take into account the distinct attributes of the threat as well as characteristics of international law and lawmaking. With facilities relying more and more on computer systems to carry out a range of tasks – from business networks to monitoring and control of operations – and adversaries becoming more sophisticated, vulnerabilities to cyber attacks in the nuclear sector are increasing. National borders do not confine the origins and effects of cyber attacks on nuclear facilities, potentially resulting in theft of material or sabotage of the facility. This means that addressing these threats requires an international approach.

Particular aspects of cyber threats in the nuclear sector impact possible international legal approaches to the issue. First, cyber threats are a relatively recent phenomenon, and the means and methods of carrying out cyber attacks are still evolving. The technology is such that non-State actors, as well as States, are capable of doing significant damage. At the same time, the treaties that make up the international legal framework were developed at a time[1] when such threats were not yet considered. Second, and related to this, modern computer networks and

[1] The Convention on the Physical Protection of Nuclear Material (CPPNM) entered into force in 1987. Both the CPPNM Amendment and the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT) were discussed and/or negotiated starting in the late 1990s, and both were adopted in 2005. ICSANT entered into force in 2007, a year that saw cyber attacks on Oak Ridge National Laboratory in the U.S., Estonian banks, ministries and parliament, and U.S. government agencies, among others.

systems are complex, and complexity often breeds vulnerabilities. Third, vulnerabilities when it comes to nuclear facilities can lead to the release of radiation. This would be the most extreme scenario, but several other possibilities exist, such as theft or compromise of sensitive information, compromise of systems for physical security allowing for access to and/or theft of material, among other scenarios. Fourth, there are sophisticated adversaries with the will and determination to cause damage, harm and panic on a massive scale, making nuclear facilities attractive targets. Adding this up, it is clear that international action is needed to prevent, detect and respond to cyber attacks as part of the broader nuclear security regime.

The problem is that modifying existing international law or adopting new legal instruments is a cumbersome process, as demonstrated by the difficulties encountered with getting the CPPNM Amendment entered into force, suggesting that this approach is not necessarily fit for addressing evolving, technologically complex threats. The international legal framework, though, is more than just a set of binding obligations for which States can be held responsible. It also, for instance, creates mechanisms for sustained interaction among States and, in the case of the nuclear security framework, provides for the development of guidelines under the auspices of the IAEA to help strengthen domestic nuclear security regimes. This latter element, which takes the form of legally non-binding instruments, should be the focus of actions, at least in the short-term, aimed at the development of the international legal framework to better address cyber threats.

2. Structure of the International Legal Framework for Nuclear Security

The international legal framework for nuclear security is comprised of two categories of instruments – legally binding and legally non-binding. On the legally binding side, there are the relevant treaties, namely the CPPNM [1], and its 2005 Amendment [2], and ICSANT [3], as well as pertinent UN Security Council Resolutions – 1540, 1977 and 1373. The CPPNM requires States parties to implement benchmark levels of physical protection with respect to nuclear material used for peaceful purposes while in international transport. In addition, the CPPNM obliges States parties to make the commission, the threat or attempt to commit and participation in certain offenses punishable under national law. The CPPNM, thirdly, contains provisions for international cooperation involving, inter alia, information exchange and coordination of recovery and response operations. The 2005 Amendment, when it enters into force, will generally broaden the scope of the treaty. It requires the application of physical protection measures to nuclear material in domestic use, storage or transport and to nuclear facilities. It also lays out fundamental principles of physical protection,[2] mandates increased international cooperation and adds the criminal offense of sabotage of nuclear material or a nuclear facility, which is particularly important with respect to cyber threats.

ICSANT, on the other hand, primarily focuses on criminalization. In the context of the overall legal framework, ICSANT adds offenses involving activities with radioactive material other than nuclear material to the list of international crimes, as long as they are accompanied by the requisite intent to cause death or serious bodily injury or substantial damage to property or to the environment. With respect to physical protection, ICSANT requires States "to make every effort" to ensure protection of all radioactive material, thereby taking into account IAEA recommendations.

[2] These fundamental principles mirror, though are not identical to, the essential elements of a State's nuclear security regime as contained in IAEA Nuclear Security Series No. 20, 2013, Objective and Essential Elements of a State's Nuclear Security Regime.

The Security Council resolutions mentioned above are binding on all member States of the UN and therefore are, as opposed to the relevant treaties, universal. Pursuant to Resolution 1540 States must develop and maintain appropriate effective measures to account for and secure nuclear material in production, use and storage as well as appropriate and effective physical protection measures, border controls and export controls, among other actions. Resolution 1977 follows from Resolution 1540 and goes into more detail in terms of implementation assistance activities to be carried out by the 1540 Committee – established to oversee implementation of the Resolution – in cooperation with States, international, regional and sub-regional organizations. Resolution 1373 is also relevant here as part of the pantheon of UN counter-terrorism measures.

On the legally non-binding side are various instruments primarily developed under the aegis of the IAEA. In this category are the fundamentals and recommendation-level documents of the Nuclear Security Series (NSS), supplemented by the technical guidance and implementing guides that are similarly part of the NSS hierarchy. The NSS elaborates and provides guidance on national implementation of essential nuclear security elements. The recommendation-level documents – namely NSS 13 [4], otherwise known as INFCIRC/225/Rev.5, and NSS 14 [5] – are explicitly designed, in part, to be consistent with and help States in implementing their obligations under relevant treaties, the CPPNM as amended and ICSANT, respectively. Aside from the NSS, the Code of Conduct on the Safety and Security of Radioactive Sources (Code of Conduct) generally aims, inter alia, to achieve a high level of security of radioactive sources through the "establishment of an adequate system of regulatory control of radioactive sources, applicable from the stage of initial production to their final disposal, and a system for the restoration of such control if it has been lost." The development process for the Code of Conduct was different than for the NSS documents, and States have been called upon to express their political commitment to the Code of Conduct in writing. To this point 125 States have done so. The IAEA continues to develop practical guidance on complying with the Code of Conduct, including the Guidance on the Import and Export of Radioactive Sources (Import/Export Guidance), and to foster and facilitate information exchange on, for instance, lessons learned with respect to implementation of the Code of Conduct. NSS 14 will also assist States in implementing their Code of Conduct commitments.

3. Provisions of Treaties Applicable to Computer Security[3]

Neither of the main nuclear security treaties makes direct reference to computer security nor to criminalization of cyber-related offenses. However, each contains provisions applicable to a certain extent to combatting cyber threats. The CPPNM Amendment requires States parties to generally protect against theft of nuclear material and sabotage of nuclear material and nuclear facilities based on the State's current evaluation of the threat.[4] Such measures should, of course, encompass securing computer networks and systems as necessary. The CPPNM Amendment also requires the criminalization of offenses related to sabotage of nuclear material or a nuclear facility. Sabotage as a criminal offense under the CPPNM Amendment entails the intentional commission of acts against a nuclear facility, or acts interfering with the operation of nuclear facilities where the offender intentionally causes, or where the offender knows that the act is likely to cause, death or harm to people, property or the environment.[5] The death or harm must be caused by exposure to radiation or release of radioactive

[3] Following the lead of NSS 17, this paper considers computer security and cyber security to be synonymous.
[4] Article 2A, paragraph 1 and Fundamental Principle G.
[5] Article 7, paragraph 1(e).

substances. Built in to the definition of "nuclear facility" in the CPPNM Amendment is the qualification that damage thereto or interference therewith could lead to the release of *significant* amounts of radiation or radioactive material. In contrast, pursuant to ICSANT, it is a criminal offense to damage a nuclear facility in such a way as to cause or risk the release of *any amount* of radioactive material. Though differing in scope, each of the offenses related to sabotage under these two treaties is broad enough to cover cyber attacks. Under ICSANT, such cyber attacks must have been carried out with the specific intent to cause death or damage to human health, property or the environment, and in a manner that releases or risks the release of radioactive material through the damage.[6]

The focus of this paper thus far has been on the instruments that are part of the nuclear security legal framework. Aside from these instruments, though, it is important to include the Cybercrime Convention [6], which aims to address cyber threats more generally. The Cybercrime Convention is the first, and still only, international treaty that specifically deals with computer-based crimes. In terms of possible application in the nuclear sector, the convention establishes offenses related to accessing without right the whole or any part of a computer system, interfering with computer data and interfering with the functioning of a computer system.[7] However, the Cybercrime Convention is really at this point a regional treaty, with the parties thus far limited to member States of the Council of Europe and seven non-member States, though it is open to all States.

To sum up this section, the treaty law is clearly limited when it comes to addressing cyber threats in the nuclear sector. It is limited in terms of scope, number of parties and/or precision of commitments.

4. Role of Non-Binding Instruments: Nuclear Security Series

Legally non-binding instruments are particularly important in the area of nuclear security where there is a recognized need for harmonized actions to prevent malicious acts involving nuclear and other radioactive material and related facilities while sensitivities and the need for precision impacts the extent to which States are willing to enter into binding obligations. Non-binding instruments provide flexibility. They can be adopted more rapidly, and amended or replaced relatively quickly if they do not meet current needs [7]. An example of this is INFCIRC/225, which has been updated a number of times since 1975 to take into account changing circumstances. In a sector where development of technologies and the related evolution of threats occur fairly rapidly, such flexibility is essential for continued viability of the framework. Non-binding instruments can also provide substantially more detail or precision to fill in for the limitations of the treaty regime. This determinacy, which is often not achievable in multilateral treaty negotiations, can lead to more harmonization by reducing State-by-State interpretation and discretion when it comes to measures taken. This contributes to effectiveness.

Because they are non-binding, States are not legally obligated to act in accordance with these instruments. This should not be mistaken for them having no legal effect, however. It could be expected that treaties have a stronger compliance pull, as States become party through a process that gives the treaty legal effect in domestic legislation. However, by virtue of the development process of Nuclear Security Series documents – developed by experts from IAEA member States in collaboration with the IAEA Secretariat and culminating in a 120-day

[6] Article 2, paragraph 1(b).
[7] Articles 2, 4 and 5.

review period for all member States – they reflect broad international agreement and are often considered standards. One could argue that general acceptance of such instruments can serve to legitimize conduct in accordance with them and make it more difficult to maintain the legality of opposing positions, or that eventually such instruments may even provide evidence of State practice or *opinio juris* required to demonstrate that a rule has become customary law [8].[8] In the specific case of the NSS documents, the development process serves to increase compliance pull, as one can see in examining the extent to which the recommendations, in particular INFCIRC/225, are reflected in domestic systems. Resulting in adoption or modification of domestic legislation and regulations means that these instruments do have legal effect, while the instruments themselves remain non-binding.

Taking this proposition a step further, at the 2014 Nuclear Security Summit in The Hague, 35 participating States pledged to reflect the NSS fundamentals and recommendation-level documents in their national systems through, inter alia, the implementation or enhancement of national regulations. The Joint Statement containing this pledge, which has now been circulated to IAEA member States as INFCIRC/869, couples legislative and regulatory actions with the commitment to host international reviews, such as International Physical Protection Advisory Service missions (IPPAS), periodically and to act on the recommendations that come out of the reviews in order to continuously improve the effectiveness of national nuclear security regimes [9]. While this does not change the non-binding nature of the documents, nor was that the intention, this commitment is indicative of the top two tiers of NSS documents being seen as international standards.[9]

The non-binding instruments, as well as the relevant treaties and Security Council Resolutions, must be seen not in isolation but as part of the broader international nuclear security framework, which means that the relationship between the two categories of instruments is essential. Under the Nuclear Safety framework, for instance, the relationship is made explicit in the legally binding instruments. Both the Convention on Nuclear Safety [10] and the Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management [11] make direct reference to the international standards,[10] invoking them as guidance on how parties can achieve the object and purpose of the conventions. For the Joint Convention, the international standards are invoked as guidance for fulfilling specific obligations.[11] In both of these cases the legally non-binding instruments are expressly included because of the additional detail and timeliness – reflecting current approaches – they provide. Put another way, in these cases the non-binding instruments serve to complement the treaties.

There are similarly certain cross-references in the nuclear security treaties. The CPPNM Amendment preamble, in a nearly identical formulation as that found in the Convention on Nuclear Safety, recognizes the guidance provided by the non-binding instruments with respect to contemporary means of achieving effective physical protection. ICSANT makes reference to IAEA recommendations in regard to physical protection of radioactive material in general and when it is seized or taken control of following a criminal act.

---

[8] It should be pointed out that the NSS recommendations are formulated as suggested actions instead of obligations, using the term "should" instead of "shall".

[9] U.S. Secretary of Energy Ernest Moniz, in announcing the Joint Statement at the 2014 Nuclear Security Summit, referred to the documents as "the closest thing we have to international standards for nuclear security."

[10] These references are found in the preambles to both treaties.

[11] Articles 4 and 11.

It is also possible that non-binding instruments serve as precursors to treaties. Such was the case for the Convention on Early Notification [12]. Existing guidelines facilitated its rapid adoption following the Chernobyl accident.[12]

When it comes to cyber security in the nuclear sector, making use of non-binding instruments would be an alternative to lawmaking, at least in the short-term. The threat is contemporary and evolving, and approaches to cyber security at nuclear facilities, as is indeed the case for cyber security more generally, are still developing. Yet, there is a need for clear international guidelines that States can follow to ensure sufficient computer security, which will also help build confidence among States in the strength of domestic systems. This is why addressing cyber threats through the Nuclear Security Series is preferable, and more likely to be realized, than attempting to modify existing treaties or adopting a new legal instrument.

5. Approach to Addressing Cyber Threats through Revision of Recommendation-Level Documents

In general, each of the three recommendation-level documents in the Nuclear Security Series hierarchy is meant to provide guidance to States in setting up or strengthening, implementing, and maintaining their nuclear security regimes through the establishment or improvement of particular capabilities in order to reduce risks of malicious activities. The collective intent of the three sets of recommendations is to help States with setting up a "comprehensive national nuclear security regime."[13] At the moment, however, only INFCIRC/225/Rev.5 (or NSS 13) contains any reference to computer security, and then in a very limited manner. NSS 13 recommends that States secure computer-based systems used for physical protection, nuclear safety and material accountancy and control against compromise in implementing a physical protection system against both sabotage and unauthorized removal, as well as secure systems used for access control. In total, there are only three specific recommendations that deal with cyber issues.

NSS 17 [13], on the other hand, does provide specific guidance on computer security at nuclear facilities. The problem is that NSS 17 is a technical guidance document in the NSS hierarchy, which means it gives details on how to take necessary measures rather than setting out the measures themselves that should be taken to achieve and maintain an effective nuclear security regime. This latter aim is the role of the recommendation-level documents. Therefore, it makes sense to revise the recommendation-level documents to set out the measures that States should take to achieve appropriate and effective computer security. To do so, it would be possible, for instance, to elevate certain elements of NSS 17 to the level of recommendations.

As described above, there is a clear process for developing Nuclear Security Series documents and substantial experience with revising the recommendations, namely in the case of INFCIRC/225. For decades INFCIRC/225 has been the recognized basis for physical protection, and States have indicated that they follow these recommendations in their domestic regimes. Revision 6 could include recommendations on legislative considerations pertaining specifically to cyber security and recommendations on regulatory requirements,

[12] INFCIRC/321, Guidelines on Reportable Events, Integrated Planning and Information Exchange in a Transboundary Release of Radioactive Materials.
[13] Paragraph 1.6 of NSS 13 (INFCIRC/225/Rev.5) and NSS 14, and paragraph 1.8 of NSS 15.

such as making computer security part of the site security plan, or more specific requirements on review and enforcement processes when it comes to computer security policy.[14]

Among other things, bringing cyber security more integrally into INFCIRC/225 will put the issue more squarely in the realm of IPPAS missions. IPPAS missions look at a State's physical protection system in light of international guidelines, i.e. currently INFCIRC/225/Rev.5, and recognized best practices. These voluntary reviews (a category which also includes, for instance, International Nuclear Security Service missions) represent the only international assessment of the establishment and implementation of a State's nuclear security regime. Though IPPAS missions to date have already made suggestions to States regarding cyber security, cyber security is not at a sufficiently high level in the Nuclear Security Series hierarchy for detailed assessment as part of IPPAS missions. Cyber security at the recommendation level will give IPPAS missions more authority to assess and make recommendations on national measures in this area.

Because INFCIRC/225 only covers nuclear material and nuclear facilities, computer security should similarly be incorporated into NSS 14 and NSS 15 [14]. NSS 17 only provides guidance on computer security at nuclear facilities. Computer security as it pertains to other radioactive material and related facilities must therefore also be considered and, if needed, measures specific to such material and facilities should be defined. By taking this approach, States will have clear guidelines for how to incorporate cyber security into their broader national nuclear security regimes, the implementation of the measures can be better assessed by peer reviews, and the resulting harmonization of measures will build confidence in the effectiveness of national regimes to deal with cyber threats.

6. Conclusion

Considering the vulnerabilities of computer systems to cyber attacks and the related threat scenarios specific to the nuclear sector, there is a pressing need to develop the international legal framework for nuclear security to better address cyber threats distinct to the nuclear field. Adaptation of the Nuclear Security Series recommendation-level documents is a good place to start, certainly when considering the evolving nature of the threat, the challenges of international lawmaking and the shortcomings of international "hard law" in technically complex areas. These non-binding instruments provide the needed flexibility and technical detail to deal with emergent and still developing threats. In this way, the non-binding instruments could further supplement the scope of the relevant treaties, which either focus on criminalization or generally require protection against theft or sabotage without added guidance on how to do so. Taking this path can also help build commitment to certain harmonized actions aimed at addressing cyber threats, thereby facilitating, if necessary, eventual codification in "hard law".

In the longer term, it would be advisable also to take up cyber security in the context of the CPPNM. A CPPNM review conference will be mandated five years after entry into force of the 2005 Amendment. Pursuant to Article 16, such conferences are meant to review not only implementation of the convention, but also its adequacy "as concerns the preamble, the whole of the operative part and the annexes in light of the then prevailing situation." Cyber threats are likely to remain part of the prevailing situation for the foreseeable future, which means the issue should be taken up in a CPPNM review conference. Having cyber security guidance in

[14] These measures are derived from NSS 17.

place in the Nuclear Security Series recommendation-level documents will allow the States parties to the CPPNM, for instance, to adopt a common understanding of "protection against theft of nuclear material and sabotage of nuclear material and nuclear facilities" that includes cyber security along with a common approach to addressing cyber threats that involves the implementation of the IAEA guidance. This further integration of the legally binding and non-binding instruments can be expected to strengthen the international legal framework for nuclear security.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, *Convention on the Physical Protection of Nuclear Material*, Legal Series, no. 12, 1979.

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, CPPNM/AC/CoW/SR.2, *Amendment to the Convention on the Physical Protection of Nuclear Material*, IAEA international law series, no. 2, 2006.

[3] UNITED NATIONS, *International Convention for the Suppression of Acts of Nuclear Terrorism*, United Nations Treaty Series, vol. 2445, 2007.

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, *Nuclear Security Series No. 13*, INFCIRC/225/Revision 5, 2011.

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, *Nuclear Security Series No. 14*, 2011.

[6] COUNCIL OF EUROPE, *Convention on Cybercrime*, Budapest, November 2001.

[7] SHELTON, D., *Commitment and Compliance,* 2000.

[8] BOYLE, A. and CHINKIN, C., *The Making of International Law*, 2007.

[9] HERBACH, J., "The Nuclear Security Implementation Initiative: A Catalyst for Needed Actions," *Arms Control Today*, no. 5, June 2014.

[10] *Convention on Nuclear Safety*, 1963 UNTS 293 (1994).

[11] *Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management*, United Nations Treaty Series, vol. 2153, no. 37605.

[12] *Convention on Early Notification of a Nuclear Accident*, 1457 UNTS 133 (1986).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, *Nuclear Security Series No. 17*, 2011.

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, *Nuclear Security Series No. 15*, 2011.