National Security Law

James D. Carlson
Geoffrey Goodale
Guy C. Quinlan
Sergio L. Suarez

Recommended Citation
James D. Carlson et al., National Security Law, 50 ABA/SIL YIR 499 (2016)
https://scholar.smu.edu/til/vol50/iss0/35

This Article is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in International Lawyer by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.
National Security Law

JAMES D. CARLSON, GEOFFREY M. GOODALE, GUY C. QUINLAN,
AND SERGIO L. SUAREZ*

This article surveys 2015 developments in National Security Law relevant to international lawyers.¹

I. Cybersecurity Developments

Several important cybersecurity developments have occurred during the past year. As discussed below, these included three main developments: (i) the enactment of several cybersecurity-related laws; (ii) the implementation of regulations requiring certain kinds of government contractors to disclose when significant cybersecurity breaches have occurred under certain circumstances; and (iii) the promulgation of an Executive Order that would permit the President to impose sanctions on foreign entities found to have engaged in cyber-attacks on U.S. persons.

In December 2014, several cybersecurity-related bills were passed by Congress and signed into law by President Obama. The Cybersecurity Work Force Assessment Act requires the Director of Homeland Security, within 180 days after enactment of the law and annually thereafter for three years, to conduct an assessment of the cybersecurity workforce of the U.S. Department of Homeland Security (DHS).² The National Cybersecurity Protection Act of 2014 amends the Homeland Security Act of 2002 to establish the National Cybersecurity and Communications Integration Center (Center) in DHS to carry out the responsibilities of the DHS Under Secretary responsible for cybersecurity.

¹. For developments during 2014, see James D. Carlson et al., National Security Law, 49 ABA/SIL YIR (n.s.) 373 (2015).
overseeing critical infrastructure protection, cybersecurity, and related DHS programs; requires the Center to be the federal civilian interface for sharing cybersecurity risks, incidents, analysis, and warnings for federal and non-federal entities; and directs the center to enable real-time, integrated, and operational actions across federal and non-federal entities.\(^3\) The Cybersecurity Enhancement Act of 2014 provides for the establishment of ongoing, voluntary public-private partnership to improve cybersecurity and authorizes the U.S. Government to support research, raise public awareness of cyber risks, and improve the nation’s cybersecurity workforce.\(^4\)

In addition to the laws referenced above, cybersecurity-related provisions are included in the Consolidated and Further Continuing Appropriations Act, 2015 (CFCAA), which President Obama signed into law on December 16, 2014,\(^5\) and the National Defense Authorization Act for Fiscal Year 2015 (NDAA), which President Obama signed into law on December 19, 2014.\(^6\) Pursuant to section 515 of the CFCAA, the U.S. Department of Commerce (DOC), the U.S. Department of Justice (DOJ), the National Aeronautics and Space Administration (NASA), and the National Science Foundation (NSF) must assess the risk of cyberespionage or sabotage before acquiring “high-impact” or “moderate impact” information technology systems (Covered Information Systems). The groups must utilize criteria developed by the National Institute of Standards and Technology (NIST) and they must review supply chain risk from the presumptive awardee against available threat information provided by the Federal Bureau of Investigation (FBI) and other federal agencies.\(^7\) Separately, pursuant to section 1632 of the NDAA, the U.S. Department of Defense (DOD) is mandated, within ninety days of the NDAA’s enactment, to establish procedures requiring the reporting of cyber incidents related to networks and information systems of “operationally critical contractors” (i.e., a contractor defined under the NDAA as a contractor designated by the DOD as “critical source of supply for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation”).\(^8\) Such procedures were ultimately promulgated in August 2015 and are discussed below.

With Congress experiencing some difficulty in passing strong cybersecurity legislation in 2015,\(^9\) the Executive branch sought to fill the void by taking several assertive actions.

---

7. CFCAA, supra note 5, § 515.
8. NDAA §632.
For example, pursuant to the requirements of section 1632 of the NDAA, and due in part to massive cyber-attacks suffered by the Office of Personnel Management (OPM) during the Summer of 2015 that resulted in sensitive data of more than 22 million current and former U.S. Government employees and applicants being hacked, the DOD issued an interim rule designed to enhance its cybersecurity posture. Under the interim rule, which became effective on August 26, 2015, all DOD contractors and subcontractors that may have “covered defense information” residing or transiting their systems are required to (1) have “adequate security” consistent with the requirements set forth in NIST Special Publication 800-171, unless a special variance is obtained from the DOD; (2) report any cyber incidents “rapidly” to DOD and to provide it significant information about their systems if the DOD opens an investigation into any such incident; and (3) implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the DOD’s Cloud Computing Security Requirements Guide if cloud computing services are going to be used by the contractor in connection with the performance of a contract with the DOD.

President Obama also sought to improve the U.S. government’s cybersecurity posture when he signed Executive Order 13694 of April 1, 2015. Under this order, sanctions can be imposed against three basic categories of designated individuals or entities. One category relates to those that take part in “cyber-enabled activities” from outside the United States that “are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.” A second category pertains to those that are:

[R]esponsible for or complicit in, or to have engaged in, the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of trade secrets misappropriated through cyber-enabled means, knowing they have been misappropriated, where the misappropriation of such trade secrets is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.

In addition, anyone who provides material assistance, sponsorship, or financial, material, or technological support, or goods or services in support of any of the targeted activities may be subject to sanctions. Furthermore, U.S. persons are generally prohibited from engaging in any dealings with entities designated under the order and any

sharing of information about cybersecurity threats). However, at the time of this writing, none of these three bills seemed likely to be passed by the other chamber of Congress and signed into law by President Obama.

14. Id.
15. Id.
16. Id.
property or property interests of such designated entities within U.S. jurisdictions or held by U.S. persons must be blocked.17

II. Nuclear Arms Control

In 2015, the United States and Russia continued to accuse each other of violating their obligations under the Intermediate Nuclear Forces (INF) Treaty,18 which prohibits the development, possession, or testing of ground-launched cruise missiles (GLCMs) with a range capability of 500 to 5,500 kilometers or of launchers for such missiles. In its 2015 Compliance Report,19 while stating that implementation of the New START Treaty20 was progressing well, the State Department again asserted that a GLCM developed by Russia is prohibited under the INF treaty, and denied Russian allegations that some aspects of the U.S. missile defense and armed unmanned aerial vehicle programs violate the INF treaty. Neither the United States nor Russia has indicated an intention to withdraw from the treaty.21 The State Department Compliance Report states that continued adherence to the INF Treaty is in “the mutual security interests of all the Parties,” and that the United States “will continue to pursue resolution of concerns with Russia,”22 while the Russian Foreign Ministry called for “businesslike” and “substantive” discussions to resolve the disputes.23

The 2015 Review Conference on the Nonproliferation Treaty (NPT)24 ended without agreement on a Final Document.25 The Conference was marked by “severe and intensifying” conflict between the five nuclear weapons states recognized under the treaty26 and a majority of non-nuclear weapons states over implementation of the obligation under Article VI of the NPT, “to pursue negotiations in good faith on effective measures relating to the cessation of the nuclear arms race at an early date and to nuclear

17. Id.


22. 2015 Arms Control Report, supra note 19.


disarmament."27 By the conclusion of the conference, 107 non-nuclear weapons states had signed a "Humanitarian Pledge,"28 originated by Austria, urging all parties to the NPT to "pursue effective measures to fill the legal gap for the prohibition and elimination of nuclear weapons."29 While some international law experts argue that actual use of nuclear weapons would violate the existing principles of international humanitarian law, e.g., the requirement of discrimination between military and civilian targets,30 the Manual of the Law of War, issued by the U.S. Defense Department in June 2015, argues that the legality of nuclear weapon use would depend on the circumstances.31

In 2015, the First Committee of the U.N. General Assembly32 voted to establish an Open Ended Working Group, open to all countries and not required to proceed by consensus, for the purpose of "taking forward multilateral nuclear disarmament negotiations."33 The resolution passed by a vote of 131 to 22 with 28 abstentions and despite all 5 P5 nations voting against it.34

The nuclear powers continued modernization of their nuclear forces in 2015. The U.S. plan includes a new fleet of nuclear missile submarines, new penetration bombers and air-launched cruise missiles, and a review of options for a new generation of intercontinental ballistic missiles (ICBMs).35 Russia announced plans for an improved, new generation of ICBMs, new bombers, and new land and sea-launched cruise missiles.36 China slightly increased the size and substantially increased the capabilities of its arsenal, replacing older missiles with improved versions.37 Pakistan38 and India39 both modernized and

34. Id.
quantitatively expanded their nuclear arsenals. Pakistan also continued development of smaller tactical warheads to deter a possible conventional arms invasion by India despite U.S. concerns that this could increase the risk of nuclear escalation.40

The Comprehensive Test Ban Treaty (CTBT)41 has not yet entered into force, although all nuclear-armed states except North Korea continued to observe a moratorium on testing. According to its terms, entry into force requires that it be ratified by a specified list of countries, including six nuclear powers that have not yet done so.42 On October 21, 2015, the U.S. State Department announced that it would begin a renewed drive for ratification but did not specify a timeline.43

In 2015, the FBI cooperated with Eastern European police in several arrests of smugglers from the former Soviet Union seeking to sell radioactive material to Middle Eastern extremists.44 On July 31, 2015, the United States completed its ratification of the Amended Convention on the Physical Protection of Nuclear Material.45 In August 2015, the White House, citing “nuclear terrorism” as “the most immediate and extreme threat to global security,” announced plans for a fourth Nuclear Security Summit to be held in Washington in 2016 on steps to secure vulnerable nuclear material and to disrupt nuclear smuggling.46

The Republic of the Marshall Islands (RMI) continued to press the suit it filed in 201447 in the International Court of Justice (ICJ) against the world’s nuclear powers.48 The suit alleges that the nuclear-armed states have breached their obligations under customary international law and, as to the five NPT signatories under Article VI of that treaty, failed...
III. International Response to Iran’s Nuclear Program

On July 14, 2015, the P5+1 (otherwise termed the E3/EU+3) and Iran agreed to a final accord addressing Iran’s nuclear program. Coined the Joint Comprehensive Plan of Action (JCPOA), it represents the culmination of twenty-two months of talks, which began in 2012 with backchannel diplomacy facilitated by Oman.

The JCPOA, which, as reproduced as an Annex to U.N. Security Council Resolution 2231, runs eighty-nine pages including Annexes and attachments, has a number of features. Among them:

- The European Union and United States agree to list the entirety of their sanctions and restrictive measures against Iran, the effects of lifting those sanctions, an agreement to terminate sanctions, and a promise to refrain from re-introducing or re-imposing sanctions, without prejudice to the dispute resolution process provided for in the JCPOA.
- Iran agrees:

50. Id.
51. Id.
52. Id.
54. This brief overview may be read in conjunction with the last three Year-in-Review articles from the National Security Law Committee, National Security Law, 49 ABA/SIL (n.s.) 373 (2015), National Security Law, 48 ABA/SIL (n.s.) 474 (2014), and National Security Law, 47 ABA/SIR (n.s.) 456 (2013).
55. The “P5+1” was coined to signify the five permanent members of the U.N. Security Council plus Germany. The group is also referred to as the “E3/EU+3,” signifying the three involved EU nations (i.e., Germany, United Kingdom, France) plus the United States, Russia, and China. Both terms are used depending on the media source.
59. Annex II, sections A and B respectively.
60. JCPOA A.26, Annex II.
To limit uranium enrichment and uranium enrichment-related activities for eight years, to be followed by a gradual evolution to the next stage of enrichment activities for exclusively peaceful purposes. To limit centrifuge operations, development, and manufacturing. Centrifuges are capped at 5,060 first generation IR-1 machines at its Natanz Fuel Enrichment Plant (FEP) for ten years, and 1,044 IR-1 machines at its Fordow Fuel Enrichment Plant for fifteen years. Its more advanced machines will be permitted in numbers varying from one to thirty, depending on the type, for testing.

To convert the Fordow facility into a nuclear, physics, and technology center.

To keep its uranium stockpile under 300 kilograms of up to 3.67% uranium hexafluoride (UF6) for fifteen years.

To permit the International Atomic Energy Agency (IAEA) a long-term presence for at least fifteen years, to permit the IAEA to implement "continuous monitoring . . . to verify that stored centrifuges and infrastructure remain in storage," and to permit the IAEA regular access, including daily access to relevant buildings at Natanz.

The parties agree to establish a Joint Commission to monitor the JCPOA implementation.

The parties agree to a conceptual redesign and subsequent rebuilding of the Arak heavy water research reactor "to support peaceful nuclear research and radioisotope production for medical and industrial purposes." The redesign will "minimize the production of plutonium and not produce weapon-grade plutonium in normal operation." The parties agreed to their respective roles in the reactor redesign, and agreed to create a document that lays out their respective roles in greater detail.

The JCPOA includes an Implementation Plan, included as Annex V to the JCPOA, describing the required sequence of actions. “Implementation Day,” i.e., the day most

62. JCPOA ¶4, Annex I §§ F, G, K, R.
64. Annex I, § H. This is down from 2,710. IAEA Doc. GOV/2014/58, supra note 63, n. 39.
65. Annex I, § G.
66. JCPOA ¶ 6, Annex I § H.
67. JCPOA ¶ 7, Annex I § J.
68. Annex I, § N.
69. Annex I, ¶ 70.
70. Annex I, ¶ 71.
71. Annex IV.
73. Annex I ¶ 2.
74. Id.
75. Annex I § B.
76. Bozorgmehr Sharafedin, World powers to help Iran redesign reactor as part of nuclear deal, REUTERS, (Nov. 21, 2015), http://www.reuters.com/article/2015/11/21/us-iran-nuclear-arak-idUSKCN0TFA0IK20151121#rWxf7teGHs0C8K.97.
sanctions are removed, will occur “upon IAEA-verified implementation of nuclear-related measures by Iran” described in Annex V paragraph 15, and upon completed actions by the European Union, United States, and United Nations, in paragraphs 16, 17, and 18, respectively. These actions reference specific paragraphs from Annexes I and II. The JCPOA will terminate ten years from the date the Security Council Resolution endorses the JCPOA.

The JCPOA was endorsed in U.N. Security Council Resolution 2231, which includes, inter alia,

- A United Nations Security Council agreement to terminate sanctioning resolutions and to remove “non-proliferation” as applied to the Iran nuclear issue “from the list of matters of which the Council is seized.”
- Establishing a mechanism to reestablish the sanctioning resolutions should Iran engage in behavior which constitutes a “significant non-performance of [its] commitments under the JCPOA.”
- Requesting the IAEA to monitor and verify voluntary nuclear-related measures by providing “regular updates to the IAEA Board of Governors” and U.N. Security Council.

Lastly, the IAEA and Iran concluded a Road-map to resolve “by the end of 2015... all past and present outstanding issues that have not already been resolved by the IAEA and Iran.” The remaining outstanding issues are provided in the annex of the 2011 Director’s General report (GOV/2011/65) and the possible military dimensions at the Parchin facility. The process includes Iran providing explanations on the outstanding issues by August 15, 2015, the IAEA reviewing the information by September 15, 2015, technical meetings to resolve ambiguities, and a final assessment on the issues to the IAEA Board of Governors by December 15, 2015. The parties met their targets, to include the IAEA visiting the Parchin facility for the first time in September, accepting samples from the facility collected by Iran while under surveillance, and the release of the IAEA Final Assessment.

The Final Assessment document says:

---

78. S. C. Res. 2231, supra note 58, ¶ 8.
80. Id., ¶ 3-6.
83. See IAEA, Road-map, supra note 81, ¶ 2-8.
84. Francois Murphy and Shadia Nasrallah, Samples taken at Iran’s Parchin Military Site: U.N. Nuclear Watchdog, Reuters (Sep. 21, 2015), http://www.reuters.com/article/2015/09/21/us-iran-nuclear-iaea-idUSKCN0RL0F20150921#kqQOxz1BQy8t4KF.97.
The Agency assesses that, before the end of 2003, an organizational structure was in place in Iran suitable for the coordination of a range of activities relevant to the development of a nuclear explosive device. Although some activities took place after 2003, they were not part of a coordinated effort. The [IAEA’s] overall assessment is that a range of activities relevant to the development of a nuclear explosive device were conducted in Iran prior to the end of 2003 as a coordinated effort, and some activities took place after 2003. The [IAEA] also assesses that these activities did not advance beyond feasibility and scientific studies, and the acquisition of certain relevant technical competences and capabilities. The [IAEA] has no credible indications of activities in Iran relevant to the development of a nuclear explosive device after 2009.86

Specific technologies the IAEA found to have characteristics consistent with development of a nuclear explosive device include (1) exploding bridgewire detonators,87 (2) multipoint initiation system,88 (3) computer modeling of such device,89 and (4) explosive safety arrangements inherent to testing such a device.90 However, all but the last item may have use in non-nuclear explosive applications. Related to the Parchin site, the IAEA assessed the extensive modifications at a particular area within the Parchin site “seriously undermined the [IAEA’s] ability to conduct effective verification.”91

IV. Surveillance and Privacy

A. United States’ Legislation

On June 2, 2015, President Barak Obama signed into law the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (“USA FREEDOM Act of 2015”).92 The new law significantly reformed the existing surveillance apparatus, which had fallen victim to scrutiny following the revelations made by former National Security Agency (NSA) contractor Edward Snowden. Following the leaks, Section 215 had been at the center of contentious litigation in the federal courts. The law revitalized Section 215 of the PATRIOT Act, but added significant restraints. Most notably, Congress ended the NSA’s controversial bulk collection program and added mandatory additional oversight of U.S. surveillance activity.93 Additionally, the law limited the government’s methods in collecting telephone metadata and added new transparency measures regarding intelligence collection.94 The USA FREEDOM Act also requires phone companies to maintain phone records, which the government could query if they receive intelligence of a specific potential threat.95

86. Id., ¶¶ 84, 85.
87. Id., ¶ 40.
88. Id., ¶ 44.
89. Id., ¶ 62.
90. Id., ¶ 67.
91. Id., ¶ 57.
93. Id.
95. Id.
The law also grants authority "to continue the acquisition of foreign intelligence information . . . [for] a period not to exceed 72 hours" without a court order.\textsuperscript{96}

\textbf{B. Surveillance Litigation in the United States}

Prior to the lapsing of Section 215 of the Patriot Act, various courts questioned the statutory interpretation underpinning the U.S. surveillance program. In \textit{Am. Civil Liberties Union v. Clapper}, 785 F.3d 787 (2d Cir. 2015), the Second Circuit Court of Appeals ruled Section 215 of the PATRIOT Act did not authorize the bulk telephone metadata program conducted by the NSA.\textsuperscript{97} Despite this determination, the court did not specifically address the question of whether bulk surveillance violates the Fourth Amendment of the United States Constitution.\textsuperscript{98} The court acknowledged the program's potential benefit, but reasoned that, due to the extraordinary measures, Congress would have to authorize such a program explicitly.\textsuperscript{99}

When Congress passed the USA FREEDOM Act, it gave the government 180 days to discontinue the bulk surveillance program. Judge Richard J. Leon supplemented the Congressional timeline by issuing an injunction against the NSA's bulk metadata collection program in \textit{Klayman v. Obama}, 800 F.3d 559 (D.C. Cir. 2015).\textsuperscript{100} The decision in \textit{Klayman} was very narrow and applied only to specifically named Verizon customers.\textsuperscript{101} The court reasoned that the plaintiffs were likely to establish that the bulk collection program violates the Fourth Amendment.\textsuperscript{102}

\textbf{C. Surveillance in the European Union}

Following an attack on satirical newspaper \textit{Charlie Hebdo}, French lawmakers passed the Surveillance Act (May 2015), which significantly expands the measures that the government can use to conduct surveillance and specifically enables French intelligence agencies to record telephone calls and text messages using technology that stores information for later use.\textsuperscript{103} The law grants the intelligence agencies the authority to conduct warrantless surveillance, allowing "the government to monitor phone calls and emails of people suspected of connections to terrorism."\textsuperscript{104} Internet service providers

\textsuperscript{97} Am. Civil Liberties Union v. Clapper \textit{et.al}, 785 F.3d 787, 824 (2d Cir. 2015). (Highlighting that the court determined that "Congress is better positioned than the courts to understand and balance the intricacies and competing concerns involved in protecting national security and to pass judgment on the value of the telephone metadata program as a counterterrorism tool.").
\textsuperscript{98} Id. at 823-24.
\textsuperscript{99} Id. at 821.
\textsuperscript{102} Id.
必须安装“黑盒子”以捕获和分析普通互联网活动，并且“使数据可供情报机构使用。”

法律设有措施，要求用于收集情报的技术和手段应与目标成比例。106 虽然执法机关必须与法官和立法者讨论，但委员会的建议不具约束力。107

欧洲法院（ECJ），关涉美国的广泛、不加区分的监控活动，推翻了美国-欧盟安全港计划，该计划被数千家公司依赖以向美国传输个人数据。108

一位奥地利公民在了解到美国的监控活动后提出诉讼。该诉讼声称，美国的法律和实践并未充分保护被政府监控传输的数据。109

ECJ确定，美国安全港计划允许美国政府干涉，并因此侵犯了“欧盟法律下‘尊重个人生活’的基本权利”。110 在其裁决中，ECJ强调《欧洲联盟基本权利宪章》赋予成员国调查其他国家是否充分保护数据传输免受政府监控的权利。111

五、伊斯兰国

伊斯兰国（IS）114 继续其国际运动，巩固其自封的哈里发国，从其在叙利亚和北部伊拉克的领土扩张。105 该计划涉及在叙利亚和伊拉克境内发起反伊斯兰国的战斗。

俄、美、英等国打击叙利亚和伊拉克境内的伊斯兰国。俄罗斯（表面上）似乎在叙利亚反对阿萨德的任何组织中打击伊斯兰国。112

美国担心伊朗的参与。113 最终，对阿萨德政府的终结存在分歧。114
proclaiming additional provinces, or “wilyat,” in parts of Yemen, Saudi Arabia, Algeria, Libya, Egypt’s Sinai Peninsula, Pakistan, Afghanistan, and Russia. The establishment of a new province is a long and complicated procedure, and several groups who have pledged allegiance to IS have yet to be recognized as provinces. Most significant is the speed in which IS expanded from controlling territory in only Syria and Iraq, to controlling territory in eight additional nations. Of these provinces, officials characterize Libya as most significant. “Western officials familiar with intelligence reports say it is the only affiliate now operating under the direct control of the central Islamic State’s leaders.” Libya is “the hub from which [IS] project[s] across all of North Africa.” It may in fact serve as a fallback position, should IS lose its territory in Syrian and Iraq.

This accumulation of controlled territory provides a steady revenue base. Estimates of IS’s annual revenues approach US $3 billion. IS is estimated to control over US $2 trillion [sic] worth of assets. Though oil is the biggest component:

the better known of the Islamic State’s revenue sources—smuggling oil, plundering bank vaults, looting antiquities, ransom of kidnapped foreigners and drumming up donations from wealthy supporters in the Persian Gulf—have all helped make the group arguably the world’s richest militant organization. But as Western and Middle Eastern officials have gained a better understanding of the Islamic State’s finances over the past year, a broad consensus has emerged that its biggest source of cash appears to be the people it rules, and the businesses it controls.

---

2187131?rel=most-read2 (Highlighting that various entries refer to the group alternately as ISIS, ISIL, the Islamic State, DAISH, and DAESH. This contribution refers to the group as the Islamic State or IS, which is how the group refers to itself).


117. See Masi, supra note 115.


119. Id.

120. Id.


Population estimates in IS-controlled territory in Iraq and Syria alone vary from about six and a half to ten million.124

The military response to IS features most prominently in daily news reports. Since operations against the IS began on August 8, 2014, the United States has carried out 2,703 airstrikes in Syria, with the rest of the international coalition carrying out 154 in Syria.25

The United States’ air operations became a little easier after Turkey agreed to allow the United States the use of the Incirlik air base in July 2015.126 However, as of this writing, the United States has carried out no air strikes in Syria after Russia deployed SA-400 anti-aircraft missiles in the wake of Turkey’s downing of a Russian jet on November 24, 2015.127

The authority for the United States’ presence against IS in Iraq is an invitation from the Iraqi government. Indeed, Iraq “requested the United States of America . . . lead international efforts to strike ISIL sites and military strongholds, with our express consent.”128 The United States’ authority to carry out operations against IS in Syria is not clear, though it appears to be grounded in self-defense;129 and in that collective self-defense is allowed where the territorial State (Syria) is ‘unable or unwilling’ to stop the attacks itself. The authority to fight IS from a domestic United States view is also unclear. President Obama has asked Congress for an explicit authorization to use force against IS, but to no avail.130

129. David Hudson, President Obama: “We Will Degrade and Ultimately Destroy ISIL”, WHITE HOUSE BLOG (Sep. 10, 2014, 10:25 PM), https://www.whitehouse.gov/blog/2014/09/10/president-obama-we-will-degrade-and-ultimately-destroy-isil (“We will hunt down terrorists who threaten our country, wherever they are. That means I will not hesitate to take action against ISIL in Syria, as well as Iraq.”).”

VOL. 50
PUBLISHED IN COOPERATION WITH SMU DEDMAN SCHOOL OF LAW
France and the United Kingdom joined the fight against IS in Syria after the IS attacks against Paris in November 2015. This adds to the coalition members who have already joined the fight in both Syria and Iraq.

In addition to the ongoing United States-led coalition air campaign, on September 30, 2015, the Russian Parliament passed President Putin’s request to approve air strikes in Syria; within hours Russian airstrikes began. The Russian intervention is pursuant to a request by Syrian President Assad for the assistance. Though Russia initially claimed to be targeting IS, Russian Foreign Minister Sergey Lavrov clarified, stating Russia would target “all terrorists in Syria.”

Attacking IS's finances is another essential aspect to defeating IS. In an effort to thwart the IS's massive revenue-generation, twenty-six nations gathered to form the Counter ISIL Finance Group (CIFG). Co-led by Saudi Arabia, Italy, and the United States, the CIFG and its participant nations met three times to determine how to deal with the IS's finances. The CIFG Action Plan states, “the unique terrorist financing challenges posed by ISIL, and identifies and establishes key steps that Coalition members, and potentially the entire international community, should undertake to disrupt ISIL's sources of revenue, movement and use of funds, and its overall economic sustainment.” The CIFG developed an action plan at its first meeting in January, through which participating countries agreed to:

1. Prevent ISIL from accessing the international financial system;
2. Counter the extortion and exploitation of assets and resources that transit, enter, or originate from ISIL-held territory;
3. Deny ISIL funding from abroad; and
4. Prevent ISIL from providing financial or material support to foreign affiliates.

Partly in response to the IS threat, the United Nation’s Security Council passed Resolution 2199, a broad effort calling on U.N. member nations to take action to impact IS’s oil trade, address the IS’s purge, destruction, and marketing of cultural heritage in Iraq and Syria. It also impacted its kidnapping and external donations, and eliminated IS's

133. The countries that have participated in the strikes in Iraq include: Australia, Belgium, Canada, Denmark, France, Jordan, The Netherlands, and the United Kingdom and the countries that participated in Syria include: Australia, Bahrain, Canada, France, Jordan, Saudi Arabia, Turkey and United Arab Emirates. U.S. DEPT OF DEFENSE, supra note 125.
135. Id.
access to financial infrastructure, arms, and related material. In response to threats from IS and other terror groups in Libya, the Security Council passed Resolution 2214 and 2249.

VII. Other Developments

A. Foreign Terrorist Fighters

Increased international scrutiny is being paid to Western recruits joining IS, not to mention Al Nasrah and a number of the groups battling for control in Syria, Iraq, Libya, and elsewhere. Specifically, “the conflict in Syria, the successes achieved on the ground by ISIS and other jihadist groups, and ISIS's formation of a self-proclaimed caliphate have had a magnetic draw for many young Western Muslims.”

In the first half of 2015, cites reported approximately 7000 foreign fighters arrived in Syria and Iraq to join terror groups. Building on the actions of U.N. Security Council Resolution 2178, the Security Council Committee, established pursuant to Resolution 1373 (2001) concerning counter-terrorism, released two reports to assess Member States’ capacity to stem the flow of foreign terrorist fighters. The reports provide an assessment of actions taken by various countries to address this threat, it included actions taken to counter violent extremism, recruitment, and incitement to conduct terrorist acts, as well as to prevent inter-state travel by foreign terrorist fighters. International concern in relation to recruitment concerning foreign terrorist fighters found further expression in a November 2015 Interpol meeting on the subject. Members discussed the issue of


141. See U.N. Security Council, Annex, Implementation of Sec. Council resolution 2178 (2014) by States affected by foreign terrorist fighters, transmitted by letter dated 2 September 2015 from the Chair of the Security Council Comm. established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council, XX, U.N. Doc. S/2015/683 (Sep. 2, 2015), available at http://www.un.org/en/sc/ctc/docs/2015/SCR%202178%202014_EN.pdf (Defined as persons “who travel or attempt to travel to a State other than their States of residence or nationality, and other individuals who travel or attempt to travel from their territories to a State other than those States of residence or nationality, for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts, or the providing or receiving of terrorist training.”).

foreign terrorist fighters travelling from the conflict zones in Syria and Iraq and the developing conflict zone in Libya.

B. SITUATION IN THE SOUTH CHINA SEA

In late October, as part of the longstanding U.S. freedom of navigation (FON) program, the USS LASSEN and a nearby P-8A Poseidon maritime surveillance aircraft, transited along a seventy-two nautical mile loop around Chinese, Vietnamese, and Filipino territorial holdings in the Spratly Islands. But confusion exists as to whether the operation was done under innocent passage. The transit involves coming within six miles of Subi Reef, a low tide elevation which the Chinese built up. A low tide elevation does not generate a territorial sea, and if the operation was done under the concept of innocent passage, the operation could be seen as an implicit acknowledgement of the validity of a Chinese territorial sea claim around the reef. One explanation was that the transit passed within twelve miles of Thitu Island, a Vietnamese-held island that does generate a territorial sea. Similarly, a flotilla of three Chinese warships passed within twelve miles of the Aleutian Islands after a joint operation with Russia. The Chinese apparently did transit under innocent passage.

C. MIGRANT CRISIS IN THE MEDITERRANEAN SEA

The migrant crisis in the Mediterranean region reached untenable levels this year due to the ongoing crises in Syria and Libya. According to the International Organization of Migration, as of January 1, 2015, 891,989 migrants were estimated to have arrived in Europe by sea, while over 3,600 people perished crossing the Mediterranean. In partial response, the Security Council passed Security Council Resolution 2240, which authorized Member States for a period of one year to inspect, and if warranted, seize vessels on the high seas off the coast of Libya where there were reasonable grounds to suspect they were being used for migrant smuggling or human trafficking from that Sea.
country. In the discussions leading up to its passage, the Libyan representative pointed out that militias control Tripoli and the ports from which the migrant ventures depart.153

D. Boko Haram

Boko Haram, based in Nigeria, overtook the Islamic State as the world’s deadliest terror group.154 Though originally promoting its own brand of Islam, IS recently accepted Boko Haram as its Islamic State of West Africa Province. Boko Haram has staged attacks in Nigeria, Cameroon, and Chad. The United States is deploying 300 troops to Cameroon at the government’s invitation and will stay until no longer needed.155 The troops will assist in airborne intelligence, surveillance, and reconnaissance.156


156. Id.