Export Controls: A Unique Tool in the War on Terror

By Darryl W. Jackson
Assistant Secretary for Export Enforcement,
Bureau of Industry and Security
U.S. Department of Commerce

Imagine a world in which a person or organization seeking nuclear weapons could simply telephone an electronics distributor in the United States, order hundreds of electronic switches normally used for medical equipment from a catalog, and then use those switches to build a nuclear weapon without anyone asking any questions. Sound far-fetched? Not long ago, a Pakistani individual named Humayan Khan tried to do exactly that. He ordered 200 switches, known as "triggered spark gaps," from a South African electronics dealer named Asher Karni. Karni, in turn, ordered the devices from a U.S. manufacturer. These switches are routinely used in lithotripters, devices that doctors employ to break up kidney stones. But they have another principal use – triggering a nuclear detonation.

Fortunately, Special Agents of the U.S. Department of Commerce's Bureau of Industry and Security (BIS) stopped this scheme before Khan obtained any triggered spark gaps. But the question remains – in a world awash in high-technology goods and easy ways for buyers and sellers to communicate via cell phones and the Internet, how can we stop the unfettered proliferation of items that terrorists, rogue states and others can use to build weapons of mass destruction (WMD) and conventional weapons? What stops such schemes from becoming routine? What prevents anyone, anywhere in the world from simply placing a phone call or going online to obtain high-technology goods in order to build sophisticated weapons?

The answer lies in a relatively unknown body of laws and regulations known as export controls. Export controls prevent or place conditions on the export of munitions items and certain "dual-use" items – those that have legitimate civilian uses but also dangerous military applications. They are an important means of dealing with emerging challenges involving high-technology transfers, WMD proliferation and terrorism.

Geopolitical Turbulence

Victory in the Cold War and the spread of democracy across the globe were welcome events, but they were not, as some theorized, harbingers of the "end of history." Indeed, the first decade of the 21st Century has been a time of extraordinary geopolitical turbulence, revealing new, and in many ways more challenging, threats to U.S. national security. We have seen the emergence of dangerous, threatening non-state forces – most prominently, militant Islamic terrorism – which perpetrated the attacks of September 11 and continue to commit unspeakable acts all over the globe.

We have reached a point in history where WMD are no longer the province of a limited group of superpowers that are deterred from using such weapons by the principle of mutually assured destruction. Unstable regimes, aided by shadowy networks of arms merchants and proliferators, have acquired and continue to seek WMD and missile technology. Iran and North Korea fall squarely into this category, and, as recent events have demonstrated, these countries may threaten world security for years to come. These new and emerging concerns in the post-September-11 world, however, have a common element with the Cold War that preceded them. That element is the desire by our foes to obtain sophisticated U.S. technology for use in ways that threaten U.S. national security. Precisely because U.S. technology – particularly technology with military applications –is the best in the world, it is on the shopping lists of those who would do us harm.

In recognition of this dynamic, the U.S. government controls all items for export that are on the control lists of the multilateral export control regimes of which the United States is a member – the Australia Group, the Missile Technology Control Regime, the Nuclear Suppliers Group and the Wassenaar Arrangement. In general, the U.S. Department of Commerce's Bureau of Industry and Security administers export controls for dual-use goods and technologies, and the U.S. Department of State administers export controls on munitions items. The Export Administration Act of 1979, which provides the statutory foundation for dual-use export controls, first expired in 1989, was periodically renewed, and has been in lapse since August 2001. When the law is in lapse, the dual-use export control system is continued by annual

Terrorists and rogue states seek WMD and sophisticated technology to perpetrate their attacks and threaten their neighbors.

Executive Orders invoking the International Emergency Economic Powers Act.

While the Bureau of Industry and Security strives to maintain U.S. leadership in the high-technology field, without adequate controls over our technology we risk having our enemies use our technology to destroy the very institutions that developed that technology. Indeed, in December 2001, shortly after the attacks on the World Trade Center and the Pentagon, Osama bin Laden instructed his followers that they "need to seek out the nodes of the American economy and strike the enemy's nodes."

Weapons of Mass Destruction

Terrorists and rogue states seek WMD and sophisticated technology to perpetrate their attacks and threaten their neighbors. As President George W. Bush noted in his address to the 2006 graduating class at West Point, our enemies today are "seeking weapons of mass murder that would allow them to deliver catastrophic destruction to our country." The president also saw parallels between the threat we face today and those of earlier times: "If our enemies succeed in acquiring such weapons, they will not hesitate to use them, which means they would pose a threat to America as great as the Soviet Union." Osama bin Laden has stated that the acquisition of WMD is a "religious duty."

The splintered world of arms proliferators operating in the shadows, coupled with an ever-expanding list of groups and states seeking sophisticated weapons and WMD, requires heightened investigative, interdiction and law enforcement efforts. This will ensure that sensitive materials do not fall into the hands of those who would use them to threaten our national security. We recognize that the unholy nexus of terrorism and technology requires law enforcement and intelligence agencies

to broadly focus their efforts on stopping the proliferation of conventional weapons and weapons of mass destruction. That policy is enshrined in the 2006 National Security Strategy, which states that the United States Government is "committed to keeping the world's most dangerous weapons out of the hands of the world's most dangerous people." Denying our foes access to U.S. dual-use technology is equivalent to cutting the supply lines of an enemy army in a conventional war, and is the essence of the mission of BIS in enforcing export controls.

In that context, we target our active investigative and enforcement efforts on the most significant threats facing the U.S. today: the proliferation of WMD, terrorism and state sponsors of terror, and diversions of dual-use goods to unauthorized uses. Since September 11, and especially over the last year, BIS has reengineered its priorities to focus to an even greater extent on preventing the spread of items, such as WMD, or other technology that is useful to terrorists whose primary goal is threaten U.S. national security.

Preventing exports of WMD

BIS's renewed focus on stopping the export of WMD and terror-related items has borne considerable fruit. For example, as discussed at the outset, BIS agents recently investigated and brought to justice an individual who was illegally exporting a dual-use item – triggered spark gaps – to Pakistan. Those items are useful in lithotripters, devices used in hospitals to treat kidney stones, but also as nuclear weapons detonators. That case was a truly worldwide undertaking, involving a U.S. manufacturer, a South African electronics distributor and a Pakistani end-user. The Pakistani end-user ordered about 200 of the triggered spark gaps through the South African dealer, falsely claiming they were intended for medical use. Triggered spark gaps are highly durable, long-lasting items, and the quantity of the Pakistani's order made it suspicious. BIS tracked an initial shipment of the triggered spark gaps. That shipment traveled from the U.S., to South Africa, then through the United Arab Emirates, before finally arriving in Pakistan. After South African police entered the dealer's offices, the dealer was arrested when he arrived in the U.S. for a vacation. He was recently convicted and sentenced to three years in prison.

BIS is also taking decisive action to restrict the export to "bad actors" of components – both those that are inherently dangerous and those that only seem more benign – that can be used in the assembly of improvised explosive devices (IEDs). Earlier this year, the United States government came into possession of information that certain electronic components were being used in IEDs against U.S. and coalition forces in Iraq and Afghanistan – items that found their way to insurgent forces through shipments to a company called Mayrow General Trading and related parties in the United Arab Emirates (UAE). In response, in June 2006, BIS published a "General Order" to the Export Administration Regulations (EAR). The General Order imposes a license requirement for exports and re-exports of all items subject to the EAR where the transaction involves Mayrow or related entities. The General Order serves two important, complementary purposes. First, it provides U.S. exporters with important information regarding Mayrow and its activities, so that exporters can ensure that proposed transactions with Mayrow are for legitimate commercial purposes. Second, it affords BIS the opportunity to review proposed transactions involving Mayrow to ensure they are in the best interests of U.S. national security and the safety of our armed forces overseas. Through this General Order, U.S. businesses and BIS can work together to ensure legitimate use of U.S. items abroad.

In addition, BIS investigations have led to the arrest and conviction of individuals exporting sensitive goods to terrorist organizations. For example, one recent case involved the export of night vision equipment to the Iranian-backed terrorist organization Hezbollah. The conflict in Lebanon in the summer of 2006 further demonstrated that the ability of terror groups, such as Hezbollah and Hamas, to obtain sophisticated weaponry threatens the stability of the Middle East. Unfortunately, these recent events also demonstrate how cunning such groups are in obtaining these weapons and underscore the importance of BIS's mission.

Heightened Surveillance

Our heightened vigilance since September 11 is evident in the multifold increase in the overall number of export violations investigated and prosecuted over the last decade. Between Fiscal Years 1996 and 2000, BIS investigations led to 24 criminal convictions and 164 administrative actions resulting in penalties. Since then, BIS efforts have dramatically increased those numbers. Between Fiscal Years 2001 and 2005, criminal convictions increased four-fold, to 95, and administrative actions resulting in penalties rose by 28 percent, to 210. For Fiscal Year 2006, BIS obtained 34 criminal convictions and over $3 million in criminal fines and 95 administrative settlements for dual-use export violations with over $13 million in administrative penalties.

Another aspect of BIS's enforcement efforts is its enforcement of U.S. antiboycott laws. These laws are primarily, but not exclusively, intended to prohibit certain conduct related to the Arab League boycott of Israel, which still exists in varying levels across the Arab world. The boycott exists on several different levels, only some of which can be countered by U.S. export control laws. U.S. companies are prohibited from taking certain actions or providing certain types of information in support of the boycott. In Fiscal Year 2006, BIS assessed administrative penalties against nine companies for violating the antiboycott laws. In addition, antiboycott violations can serve as the basis for criminal charges. A recent BIS investigation uncovered a company that assured its Syrian customer in writing that goods it was exporting "were not of Israeli origin." Furnishing this information, and failing to report the buyer's request for this information, violated the antiboycott laws. The company was convicted of these and other export control violations in a criminal case.

In sum, the dramatic changes in the world have underscored the imperative of thinking creatively and working cooperatively to ensure that sensitive goods do not fall into dangerous hands. BIS stands at the forefront of these efforts. In the post-September-11 world, export controls play a uniquely important role in maintaining our national security. We are committed to ensuring that BIS's export enforcement efforts continue to adapt to the increasingly sophisticated and dangerous security challenges facing our country.