

# Chapter 19

## International Security

# International Security

- International Disruptions
- International Organizations Efforts
- National Governments Efforts
- Corporate Efforts
- Security Approaches

# International Disruptions

Many unexpected events can cause serious disruptions in world trade. Unforeseen events include natural disasters, power outages, and terrorist attacks.

- A single eruption of an Icelandic volcano interrupted all flights in most of Europe for a week in April 2010.
- A ship stuck in the Suez Canal stopped all ocean cargo movement for a week in 2021.

None of these events are predictable.

However, some of these events are preventable and it is possible to prepare for the disruptions that they will cause.

# Turning Points

International and national terrorism have had a significant impact on many countries in the past decades. However, four events galvanized international responses:

- The World Trade Center attacks (Sept. 11, 2001)
- The Madrid train bombings (March 11, 2004)
- The Mumbai attacks on rail commuters on July 11, 2006 and on hotels on Nov. 26, 2008.
- Utoya Island massacre, on July 22, 2011.

These attacks showed that no country was immune to the problem, and pushed international organizations and governments to work together to prevent future incidents.

| <b>Major Terrorist Acts 1993 – 2012</b> |                            |                               |
|---|----------------------------|-------------------------------|
| World Trade Center Bombing              | February 26, 1993          | New York City, United States  |
| Sarin Gas Subway Attack                 | March 20, 1995             | Tokyo, Japan                  |
| Oklahoma City Bombing                   | April 19, 1995             | Oklahoma City, United States  |
| Métro Bombings                          | Summer-Fall 1995           | Paris, France                 |
| Omagh Bombings                          | August 15, 1998            | Omagh, Northern Ireland       |
| World Trade Center Attacks              | September 11, 2001         | New York City, United States  |
| Anthrax Mailings                        | September-October 2001     | United States                 |
| Bali Bombings                           | October 12, 2002           | Bali, Indonesia               |
| Istanbul Bombings                       | November 15 and 20, 2003   | Istanbul, Turkey              |
| Moscow Metro Bombing                    | February 6, 2004           | Moscow, Russia                |
| Madrid Train Bombings                   | March 11, 2004             | Madrid, Spain                 |
| London Subway Bombings                  | July 7, 2005               | London, United Kingdom        |
| Mumbai Hotel Attacks                    | November 26, 2008          | Mumbai, India                 |
| Kampala attacks                         | July 11, 2011              | Kampala, Uganda               |
| Utoya Island massacre                   | July 22, 2011              | Utoya Island and Oslo, Norway |
| Monterrey Casino attack                 | August 25, 2011            | Monterrey, Mexico             |
| Boston Marathon bombings                | April 15, 2013             | Boston, United States         |
| College campus attacks                  | April 2, 2015              | Garissa, Kenya                |
| Bataclan Theater                        | November 13, 2015          | Paris, France                 |
| Chemical attack on rebel territory      | April 7, 2016              | Aleppo, Syria                 |
| Truck rampage                           | July 14, 2016              | Nice, France                  |
| Car rampages                            | March 23, and June 3, 2017 | London, United Kingdom        |
| Mosque shooting                         | March 15, 2019             | Christchurch, New Zealand     |
| Vienna attack                           | November 2, 2020           | Vienna, Austria               |

# International Organizations

Some of the first efforts against international terrorism were led by the large international organizations:

- The International Maritime Organization (IMO)
- The Customs Cooperation Council (better known as the World Customs Organization (WCO))
- The International Chamber of Commerce (ICC)

Each of these organizations implemented measures designed to prevent further terrorist acts and improve security at ports around the world and in international trade.

Individual governments implemented their own measures, both within the frameworks provided by these organizations and independently.

# International Maritime Organization

The International Maritime Organization (IMO) implemented the International Ship and Port Facility Security (ISPS) Code in December of 2002.

This code enhances port security by requiring specific security measures that ports have to put in place, such as controlling access, monitoring activities, and having secure communication systems.

The code also recommends similar measures for merchant ships.

The IMO made ISPS part of the International Convention for the Safety of Life at Sea (SOLAS), a convention that had been ratified by many countries, so it would be implemented quickly.



**Video monitoring of port facilities is a requirement of the ISPS.**

Source: Volodymyr Kyrylyuk

# World Customs Organization

The World Customs Organization (WCO) has traditionally worked towards the “simplification and harmonization of Customs’ procedures,” but it implemented the SAFE initiative (Security and Facilitation in a Global Environment) in 2005 to combat the threat of terrorism in international trade.

The SAFE initiative attempts to coordinate the efforts of Customs offices worldwide and uses the authority of the Customs office in the exporting country to assist the customs office in the importing country to inspect cargo prior to shipment.

# The SAFE Initiative

The WCO mandates that all Customs authorities adhere to a set of advance electronic information standards for all international shipments. Each country must have consistent risk management approaches to address security threats.

Exporting countries' Customs authorities must comply with a reasonable request to inspect outgoing cargo, preferably by using non-intrusive technology (X-rays) if possible.

Customs authorities must provide benefits to companies that demonstrate minimum standards of security. Such companies are called Authorized Economic Operators and benefit from faster processing of Customs clearance and lower inspection rates.



Mobile X-Ray scanners are part of the SAFE initiative of the WCO.

Source: Rafael Ben-Ari

# International Chamber of Commerce

The International Chamber of Commerce (ICC) also weighed on the issues related to security initiatives in the domain of international logistics, in a Policy Statement dated November 2002.

In that statement, the ICC emphasized that security initiatives should be the domain of international agreements between countries, rather than initiatives imposed unilaterally by some governments.

# National Governments

Most national governments have implemented several security measures to protect their country against the threat of terrorism. Most initiatives are within the guidelines of the International Maritime Organization or the World Customs Organization, but with some variation, and some initiatives are bilateral or unilateral.

These requirements make the work of international logisticians more challenging, as they have to comply with a myriad of regulations.

# United States Programs

## **Interdiction**

The US interdiction program is based on a 100-percent inspection of luggage and air cargo. The U.S. Congress has called for 100-percent inspection of marine and road cargo, but no plan exists to implement such a measure.

The Transportation Safety Administration was created to implement this interdiction policy and so was the Department of Homeland Security.

# United States Programs

## C-TPAT

The Customs-Trade Partnership Against Terrorism (C-TPAT) is a U.S. Customs and Border Protection program in which more than 10,000 importers participate. There are three levels of participation.

Shippers that participate in the C-TPAT program have to demonstrate that they have implemented security measures in their supply chain.

In exchange, they enjoy:

- A lower inspection probability
- Priority if cargo is inspected
- Priority processing of cargo, the so-called “green lane”
- Customs’ assistance in resolving security issues

C-TPAT is based on the SAFE program of the World Customs Organization.

# United States Programs

## MTSA

The Maritime Transportation Security Act (MTSA) requires port facilities to have a security plan that includes procedures and training. It mandates equipment, such as emergency communication devices, and personnel, such as a Security Officer. The plan must be approved by the U.S. Coast Guard.

The MTSA requires ships that call on U.S. ports to have a Security Officer, and a security plan that must be approved by the U.S. Coast Guard.

The MTSA is based on the International Ship and Port Facility Security (ISPS) Code of the International Maritime Organization.

# United States Programs

## CSI

The Container Security Initiative (CSI) positions U.S. Customs officials in about 60 foreign ports. Their role is to screen and inspect containers before they are loaded onto a ship that will call on a United States port.

The CSI employs non-invasive methods of inspection, such as X-rays.

The CSI works within the SAFE framework of the World Customs Organization but has expanded it by positioning United States officers abroad.

# United States Programs

## TWIC

The Transportation Workers' Identification Credential (TWIC) program requires that all persons who have access to U.S. ports must carry an identification card.

The identification card carries biometric information and is provided after a background check. There are 2.5 million transportation workers who have acquired their TWIC credentials.

The TWIC program is broader than the ISPS initiative of the international Maritime Organization that only mandates control of the access to the port.

There has been much criticism that the TWIC program has been ineffective, because few criminal activities disqualify applicants.

# United States Programs

## ISF (10 + 2)

The Importer Security Filing (ISF or 10+2 program) requires that importers provide U.S. Customs and Border Protection with shipment data at least 24 hours before the cargo is loaded in the port of departure.

10 items are required from the importer:

1. The identification number of the importer of record (tax ID number)
2. The identification number of the consignee (tax ID number)
3. The manufacturer (name and address)
4. The seller of the goods (name and address)
5. The buyer of the goods (name and address)
6. The name and address of the business to which the shipment is going

# United States Programs

7. The stuffer's name and address (the party that filled the container)
8. The location where the container was stuffed
9. The country of origin of the goods
10. The six-digit Harmonized System number for the goods

2 items are required from the carrier:

1. The vessel stow plan (the way the containers were organized onboard the vessel)
2. The container status message (container number, location, condition—full/empty—, events—loading/unloading—, and event times)

# United States Programs

## SAFE

The Security and Accountability for Every Port (SAFE) is the name of the piece of legislation that modified some aspects of the CSI and the C-TPAT programs and created the TWIC program.

The SAFE Act of the United States shares an acronym with the SAFE program of the World Customs Organization but is entirely separate.

# United States Programs

## FAST

The Free and Secure Trade (FAST) program is a joint initiative between the Canada Border Services Agency (CBSA), the U.S. Customs and Border Protection (CBP), and Mexican Customs. It is a voluntary program.

If the exporter/importer, the carrier of the goods, and the driver are FAST participants, then the shipment can gain access to dedicated lanes at the border crossing point, for faster and more efficient border clearance.

The FAST program is based on the SAFE program of the World Customs Organization that calls for expedited clearance for Authorized Economic Operators.



The FAST lane at the US-Canada border crossing from Canada. The line would be in the center lane of the bridge.

Source: Donna Burton, US Customs and Border Protection



The FAST lane at the US-Canada border crossing from Canada.

Source: James Tourtelotte, US Customs and Border Protection

# European Programs

## **Authorized Economic Operator**

The European Authorized Economic Operator (AEO) program mirrors the WCO mandate that Customs organizations provide benefits to businesses that meet minimal supply chain security standards and best practices.

Companies involved in the international movement of can become Authorized Economic Operators after demonstrating that they have security measures in place, and having these measures reviewed and approved by their national Customs administration.

AEO status is granted to companies that have achieved Tier II of the C-TPAT requirements of the United States.

# European Programs

## Customs Security Programme

A program that requires importers to provide Customs authorities with information on goods prior to their arrival in the European Union (pre-arrival declaration).

Customs uses this information to perform a risk analysis of the shipment and enables Customs to identify high risk cargo bound for Europe. An inspection of the cargo then takes place in the port of departure, in a way that is conform to the WCO's SAFE guidelines.

European Customs authorities also inspect goods when their counterparts want them to inspect a shipment prior to loading.

# Other Countries' Programs

Other countries have implemented the International Ship and Port Facilities Security (ISPS) program of the World Trade Organization in ways that are consistent with the layouts of their ports and the types of goods they export. Therefore, a wide variety of alternatives have been implemented.

They also have implemented the Security and Facilitation in a Global Environment of the World Customs Organization and cooperate in providing pre-shipment inspections when they are requested by Customs authorities in the importing country.

# Corporate Efforts

Most companies see security issues in a much narrower way, focusing principally on the risk of theft and other criminal activities, such as tampering, vandalism, and counterfeit products, and use measures to reduce those risks.

Companies obviously comply with requests to reduce terrorism by participating in governmental programs and other efforts out of civic duty, but they mostly see the benefits of such increased security in terms of reduced cargo losses and a reduced probability of supply chain disruptions.



The two types of container seals (bolt seal on top, wire seal on bottom). Only the bolt seal is truly secure and accepted in international shipments.

Source: Pierre David

# Security Approaches

When considering inspections of in-bound cargo into a country, there are three approaches:

- Conduct a one-hundred-percent inspection of all cargo. The proponents of this method maintain that it is the safest alternative; since all cargo is inspected, nothing dangerous can possibly be shipped into the country.
- Identify potentially dangerous cargo and inspect only those shipments.
- Inspect a few randomly-selected shipments, thoroughly.

# 100-Percent Inspections

One-hundred-percent inspections consume an extraordinary amount of resources:

- Assuming that a minimum of three hours are necessary to inspect a container, and that there are roughly 20 million container shipments in international trade, the world's economies would need to hire countless inspectors.
- Assuming that containers are inspected in ports, a very large area would need to be dedicated to the inspection process. In most ports, that space is simply not available.

# 100-Percent Inspections

One-hundred-percent inspections are ineffective:

- An element of boredom makes it impossible for inspectors to be vigilant for every shipment. Audits of one-hundred-percent inspection systems (TSA's inspection of luggage, for example) have shown that many problem shipments are missed under such a program.
- Since neither the necessary manpower nor the appropriate space in port facilities can be allocated to such an inspection program, what passes for a one-hundred-percent inspection is only a cursory review of a shipment.
- Because of Type I and Type II errors, it is difficult to make one-hundred-percent inspections effective.



A bomb-sniffing machine checking passenger luggage. It commits both Type-I and Type-II errors.

Source: Piotr Redlinski

# Type I and Type II Errors

In order to understand security measures, it is important to know the two types of errors in statistics, called Type I and Type II errors. It is easier to understand these concepts by using an example.

Suppose a machine is designed to detect bombs in a piece of luggage:

There are two possible cases for the luggage:

- there is a bomb in the piece of luggage
- there is none

There are also two possible cases for the bomb-sniffing machine:

- it detects the bomb
- it does not

for a total of four possible cases.

# Type I and Type II Errors

These four cases can be arranged in the following matrix:

|                              |                                      | In the piece of luggage |                    |
|------------------------------|--------------------------------------|-------------------------|--------------------|
|                              |                                      | there is<br>no bomb     | there is<br>a bomb |
| The bomb-sniffing<br>machine | does not detect a bomb<br>(no alarm) |                         |                    |
|                              | detects a bomb<br>(alarm)            |                         |                    |

# Type I and Type II Errors

The four possibilities are:

- There is no bomb in the piece of luggage, and the bomb-sniffing machine does not detect any. This is the most common scenario.
- There is no bomb in the piece of luggage, but the machine detects one, triggering a careful manual review of the piece of luggage, that finds that there is really no bomb. This is called a Type I error on the part of the machine.
- There is a bomb in the piece of luggage, and the bomb-sniffing machine detects it, triggering a manual review that finds the bomb, hopefully without harm.
- There is a bomb in the piece of luggage, and it is so well hidden that the bomb-sniffing machine does not detect it. This is called a Type II error.

# Type I and Type II Errors

These four cases can be arranged in the following matrix:

|                              |                                      | In the piece of luggage |                      |
|------------------------------|--------------------------------------|-------------------------|----------------------|
|                              |                                      | there is<br>no bomb     | there is<br>a bomb   |
| The bomb-sniffing<br>machine | does not detect a bomb<br>(no alarm) |                         | <b>Type II Error</b> |
|                              | detects a bomb<br>(alarm)            | <b>Type I Error</b>     |                      |

# Type I and Type II Errors

Which of the two errors is more worrisome?

When asked to evaluate a bomb-sniffing machine with equal Type I and Type II error rates of 5 percent, most people conclude that the Type II error rate is most worrisome; after all, a machine that misses 5 percent of all bombs is very scary indeed.

However, in the scenario of a terrorist threat, this is an incorrect conclusion; the Type I error rate is the problem.

# Type I and Type II Errors

Suppose that there is an incidence of one bomb per one million pieces of luggage.

Let's assume a terrorist places a bomb in a piece of luggage. With a Type II error rate of 5 percent, there is a 95 percent chance that the machine will correctly detect the piece of luggage with the bomb and sound the alarm, which makes it pretty certain.

However, the machine has also inspected 999,999 other pieces of luggage prior to that day, none of which contained a bomb; nevertheless for approximately 50,000 of them, the machine rang the alarm (because it committed a Type I error) and the operator had to inspect the piece of luggage manually.

# Type I and Type II Errors

Out of the 50,000 pieces of luggage that the operator has inspected up until that day, none contained a bomb.

The single piece of luggage that contains a well-concealed bomb will not escape scrutiny; the operator will handle it with much care. However, it is also likely that the operator will assume that it is a false alarm; after all, 100 percent of the ones inspected so far have been.

The dangerous piece of luggage will then be cleared, even though the bomb-sniffing machine identified it correctly as dangerous.

# Type I and Type II Errors

Keeping these error rates at 5 percent each, and assuming that the incidence of luggage with a bomb is very small, around 0.0001 percent, the probability that a piece of luggage that is suspected to have a bomb actually has a bomb is only:

$$\frac{0.95 \times 0.000001}{0.05 \times 0.999999} = 0.002 \text{ percent}$$

In contrast, the probability that this is a false alarm is 0.998 percent.

# Type I and Type II Errors

Using this reasoning in a different context can sometimes help.

Assuming a disease that is present in 0.1 percent of the population, and assuming a test with a probability of Type-I error at 5 percent (5 percent of the population who does not have the disease nevertheless tests positive for it) and a probability of Type-II error at 0 percent (everyone who has the disease tests positive for it).

The probability of a patient who tests positive actually having the disease is:

$$\frac{0.001}{0.05 \times 0.99} = 2 \text{ percent}$$

# Inspections

When considering inspections of in-bound cargo into a country, only two approaches are effective:

- Identify potentially dangerous cargo and inspect only those shipments. That is the approach of the CSI program.
- Inspect randomly, but thoroughly, some shipments. That is the approach of Customs and Border Protection for the correct classification of goods, and this process can be expanded to inspect for dangerous shipments.