International Journal of Safety and Security Engineering
Vol. 14, No. 3, June, 2024, pp. 787-794
Journal homepage: http://iieta.org/journals/ijsse

Terrorist Attacks to Essential Services, Infrastructures and Facilities in G7 Countries During the Period 2000-2020

Marco Carbonelli[1*], Claudio Todaro[2], Vincenzo Iavarone[2], Federico Sesler[3]

[1] Presidency of the Council of Ministers, Rome I-00184, Italy
[2] O.S.S.I.S.Na., Rome I-00165, Italy
[3] CISINT, Rome I-00165, Italy

Corresponding Author Email: marcocarbonelli62@gmail.com

(This article is part of the Special Issue **SICC Series CBRNe Conference**)

https://doi.org/10.18280/ijsse.140311

Received: 20 March 2024
Revised: 19 May 2024
Accepted: 4 June 2024
Available online: 24 June 2024

Keywords:
terrorist attacks, terrorist events, global terrorist database GTD, chemical biological radiological CBR, chemical biological radiological explosive incendiary CBREI, terrorist weapons

ABSTRACT

Starting from the terrorist events recorded in the Global Terrorism Database (GTD), a very detailed and original analysis has been performed on the evolution, starting from the attach to the Twin Towers in New York in 2001, over the last 21 years of terrorist attacks on specific targets related to critical infrastructures, essential services and facilities. Specifically, a set of targets extracted from the GTD referred to in the paper as ESIF (Essential Services, Infrastructures and Facilities) macro-target has been selected to carry out an original focus on terrorist events perpetrated in G7 countries (USA, UK, France, Germany, Italy, Canada and Japan). This ESIF macro-target typically contains most of a country's strategic industrial assets, infrastructure and services. The hereby analysis has been conducted in a timely manner for the period 2000-2020, in order to carry out a comparison of the different situations recorded in the most developed world countries, to intercept possible trends, also verifying the type of weapon used for the attacks, then focusing the analysis on CBREI (Chemical, Biological, Radiological, Explosive and Incendiary) attacks, which constitute the most destructive and impactful terrorist attacks found in the GTD.

1. INTRODUCTION

For over 20 years, starting from the attack to the "Twin Towers" in New York in 2001, a global intense research and analytical activity has been performed in western countries, focusing on the topic of protection of critical infrastructures, essential services and strategic facilities [1-5] and plants through the identification of means to reduce both the risk and the impact of the effects caused by a potential terrorist attack.

Research activity on the issues of protecting these infrastructures and facilities has also led many technical bodies of institutions to produce very detailed directives and documentation in what have been considered the 'critical sectors' to be most protected from terrorist attacks. In particular, in the U.S., since 2006 the Department of Homeland Security (DHS) has produced a series of National Infrastructure Protection Plans and recommendations [4], the most recent published in 2013 [5] and cascaded 16 specific National Plans in the following critical sectors [6]: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater.

In a similar way the European Union (EU), Council Directive 2008/114/EC [7] provided at a first shared procedure for designating European critical infrastructure in the energy and transport sectors the disruption or destruction of which would generate a significant cross-border impact on at least two Member States. The most recent EU Directives, NIS2 (Network and Information Security) [8] and CER (Critical Entities Resilience) [9], define the EU framework for European critical infrastructure protection. Both NIS2 and CER Directives were enacted at the end of 2022 in the EU and need to be transposed into national law in Member States until 2024. In particular, NIS2 regulates cyber security in the EU, extending the scope and requirements for operators, while the CER Directive lays down obligations on EU Member States to take specific measures, to ensure that essential services for the maintenance of vital societal functions or economic activities are provided in an unobstructed manner in the internal market.

The non-exhaustive list of essential services to which the CER Directive applies is as follows: Energy; Transport; Banking; Financial market infrastructure; Health; Drinking water; Waste water; Digital infrastructure; Public administration sector; Space; Production, processing and distribution of food sector.

For the reasons discussed up above in this introduction, with reference to the period from 2000 to the present and starting

from the latest data collection made public by one of the world's most important databases of terrorist attacks, the Global Terrorism Database (GTD) maintained by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) and the University of Maryland [10], in this paper an analysis was conducted on the evolution of terrorist attacks on specific targets related to critical infrastructures, essential services and strategic installations. Furthermore, in light of the availability of only technical articles or more generalist articles or even devoted solely to the single State [11] with regard to terrorist attacks to critical infrastructures, the focus in this work, as discussed below, will be on all G7 countries (USA, UK, France, Germany, Italy, Canada and Japan).

Using the GTD database, in the paper the results of the number of attacks on specific targets (indicated as TargetType) are presented. Hereinafter we will define as 'macro-target' ESIF (Essential Services, Infrastructures and Facilities) the strategic industrial assets, infrastructures and services of a country, and, with reference to the GTD, this macro-target will be described by the following 8 TargetType categories: Business, Airports & Aircraft, Food or Water supply, Journalists & Media, Maritime (including ports and maritime infrastructure), Telecommunication, Transportation (other than aviation) and Utilities.

These TargetTypes, 8 in total, were selected from the 22 different TargetTypes [12] categorized in the GTD starting from the "Target/Victim Information" defined variable.

It is important to note that the ESIF macro-target, on which the analysis has been made, takes into account both attacks on structures and personnel who allow the structures themselves to function and provide the service offered.

The analysis of the above defined ESIF Macro-Target refers to the period 2000-2020 for the G7 countries, with the aim of carrying out - for this area and for this specific targets - an initial comparison between the different situations recorded in the most developed countries of the world and to intercept possible trends, also verifying the type of weapon used for the attack and focusing the analysis on CBREI (Chemical, Biological, Radiological, Explosive and Incendiary) attacks which constitute the most destructive and impactful terrorist aggressive actions mentioned in GTD.

Finally, the "Scudo Italia" Protocol has been introduced very shortly for the definition of specific anti-sabotage/anti-terrorism risk mitigation plans for ESIF macro-targets.

2. GENERAL ELEMENTS OF THE "GLOBAL TERRORISM DATABASE"

In the study, the attention has been focused on the most important international open-source database that currently describes terrorist events, the Global Terrorism Database (indicated by the acronym GTD). All the mentioned analyses have been made in accordance with the GTD terms of use, National Consortium for the Study of Terrorism and Responses to Terrorism (START), Global Terrorism Database™, University of Maryland [10, 12].

The GTD has been previously used for analyses of both general and specific nature [11, 13-17] with, for example, some early results on CBR attacks and terrorist events published in 2019 [15] and in 2021 [16] by the authors.

The 2022 available version of the GTD database, taken into consideration for the analysis presented here, includes information on terrorist events that occurred between 1970 and 2020. The database is usually updated on an annual basis.

Differently from other databases of terrorist events [13, 18], the GTD systematically and continuously includes international terrorist incidents that have occurred since 1970, with as many as fifty years of collected data to describe and characterize worldwide terrorist attacks.

The 2022 GTD available version provides information on over 200,000 terrorist attacks characterized by at least 45 variables for each case recorded in the database, with the most recent terrorist events including information on over 120 variables.

For each event reported in the GTD, the following variables are at least available: date and place of the event, brief description, used weapons, nature of the objective, number of victims and - when identifiable - the group or the responsible individual.

The information contained in the Global Terrorism Database is based on reports from various open media sources. The information - as stated by the database manager (the National Consortium for the Study of Terrorism and Responses to Terrorism, START) - is added to the GTD only if the reliability of the sources has been properly confirmed.

The START consortium that manage the GTD also provides a codebook [12] which contains all the definitions adopted and the variables recorded for each single event.

3. DEFINITION OF THE MACRO-TARGET "ESSENTIAL SERVICES, INFRASTRUCTURES AND FACILITIES"

This analysis is focused on all events of terrorist nature, also below referred simply as 'attacks' or 'events', which affected infrastructures, plants and people involved in the provision of services for those countries belonging to the G7.

The considered targets, also referred here as TargetType, are extracted from the GTD variable called Target/Victim Information, originally made up of 22 different target types [12].

Of the 22 starting TargetTypes, 8 were selected for this work. These TargetTypes are indicated in Table 1 and represent the ESIF macro-target (Essential Services, Infrastructures and Facilities).

Table 1. Macro-target ESIF

Essential Services, Infrastructures and Facilities	
TargetType (TT)	**Specific TargetType Reported in GTD**
TT1	Business
TT2	Airports & Aircraft
TT3	Food or Water Supply
TT4	Journalists & Media
TT5	Maritime
TT6	Telecommunication
TT7	Transportation
TT8	Utilities

It is important to remember that, in this analysis, the ESIF macro-target also collects attacks on personnel employed in those facilities/organizations linked to the provision of the service or the operation of the infrastructure/plant.

For further details on the ESIF macro-target, the detailed declinations (SubType) of each type of ESIF Targets are

shown in Table 2, according to the taxonomic characteristics described in the GTD codebook [12].

For the 2000-2020 time span, the analysis on the ESIF macro-target consisting of the 8 TargetTypes reported above, was conducted for the G7 countries in order to start, for this area of terrorist possible targets, a comparison between the most developed countries in the world.

Table 2. ESIF macro-target and declination in TargetSubType

ID	GTD Target Type	GTD TargetSubType
TT1	Business	Gas/Oil/Electric Restaurant/Bar/Café Bank/Commerce Multinational Corporation Industrial/Textiles/Factory Medical/Pharmaceutical Retail/Grocery/Bakery (including generic shops) Hotel/Resort Farm/Ranch Mining Entertainment/Cultural/Stadium/Casino Construction Private Security Company/Firm Legal Services
TT2	Airports & Aircraft	Aircraft (not at an airport) Airline Officer/Personnel Airport
TT3	Food or Water Supply	Food Supply Water Supply
TT4	Journalists & Media	Newspaper Journalist/Staff/Facility Radio Journalist/Staff/Facility Television Journalist/Staff/Facility Other (including online news agencies)
TT5	Maritime	Civilian Maritime Commercial Maritime Oil Tanker Port
TT6	Telecommu-nication	Radio Television Telephone/Telegraph Internet Infrastructure Multiple Telecommunication Targets
TT7	Transportation	Bus (excluding tourist) Train/Train Tracks/ Trolley Bus Station/Stop Subway Bridge/Car Tunnel Highway/Road/Toll/Traffic Signal Taxi/Rickshaw
TT8	Utilities	Gas Electricity Oil

4. ANALYSIS OF TERRORIST EVENTS ON THE ESIF MACRO-TARGET IN THE 2000-2020 TIMELINE

In this section are shown the results of the analysis of terrorist attacks on ESIF macro-target which were recorded in the GTD in the 2000-2020 timeline, in the G7 countries.

Table 3 shows both the cumulative G7 obtained results and the detail for each individual G7 country related to terrorist attacks in the 2000-2020 time span for ESIF-type TargetTypes.

In particular, the table shows the following:

- a total of 644 terrorist attacks on ESIF-type targets in the G7 countries, for the considered time span;
- in the USA and the United Kingdom was recorded the highest number of attacks on ESIF-type targets (173 events, corresponding to 26.9% of total recorded attacks);
- Italy has recorded 41 terrorist events (corresponding to 6.4% of total recorded attacks) involving ESIF type targets in 21 years;
- the country with the lowest rate of attacks on ESIF targets is Japan, with only 16 events (corresponding to 2.5% of total recorded attacks) recorded in 21 years.

Figure 1 shows, year by year in the 2000-2020 period, the number of attacks on ESIF-type targets in G7 countries. The trend shows how a peak of 75 attacks was recorded in the G7 countries in 2020, compared to a minimum value of 8 attacks recorded in 2009.

Table 3. Number of terrorist attacks on G7 countries in the 2000-2020 period for ESIF macro-target

G7 Countries	Number of Total Attacks for ESIF Macro-Target (2000-2020 Period)
USA	173
UK	173
France	151
Germany	57
Italy	41
Canada	33
Japan	16
Total	644

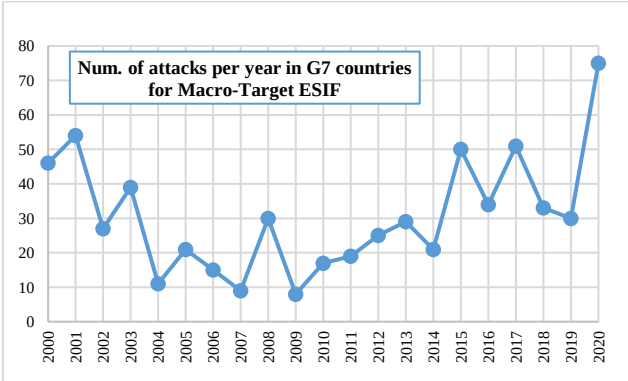

Figure 1. Number of terrorist attacks on G7 countries for each year, in the 2000-2020 period for ESIF TargetTypes

In order to display more detailed results for the G7 countries, the Table 4 shows, year by year and by individual country, the number of attacks on ESIF targets that were recorded in the GTD for the 2000-2020 period.

From this last table it can be deduced, for example, that in 2020 the United Kingdom achieved a sad record of the highest number of attacks on ESIF targets with 33 events, followed at a distance by Germany (12 events), USA (11 events), France (9 events) and Canada (8 events). Italy - with 2 attacks in 2020 - occupies the penultimate place in this attack ranking, with Japan last (with no attacks recorded).

Another important analysis that can be conducted from the data is one that characterizes, by individual G7 nation, the distribution of attacks for the TargetTypes that belong to the ESIF macro target.

In this regard, the Table 5 shows data related to the USA, which highlight - in each row of the table - the 8 TargetTypes presented in the previous paragraph.

For the case of the United States, the Table 5 shows how

out of 173 overall attacks on ESIF targets in the G7 countries, 134 are concentrated on the "Business" TargetType, 9 attacks are recorded respectively for the "Utilities" and "Journalist & Media" TargetTypes and 8 attacks are in the "Airport & Aircraft" area. Fewer attacks, however, for the "Telecommunication" (7 attacks) and "Transport" objectives (6 attacks).

Similar considerations can be made for the cases reported in the following Tables 6, 7 and 8 which show the results for the United Kingdom, France and Italy.

The results referred to attacks on "Telecommunication" targets (30 attacks) reported in Table 6 for the United Kingdom in 2020 appears to be highlighted. Also, noteworthy is the high number of events linked to "Transportation" objectives compared to the total (29 events out of a total of 173 events recorded in the 2000-2020 time span).

Table 4. Number of terrorist attacks on G7 countries for each year, in the 2000-2020 period, for ESIF macro-target

Nations/Year	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	Total
United States	19	27	5	22	3	5	2		4	4	7	2	3	5	1	8	13	13	6	13	11	**173**
United Kingdom	12	20	1	1	1	9	3	7	11		7	7	3	12	9	11	6	8	5	7	33	**173**
France	11	3	15	13	4	7	7	2	9		1	3	9	8	4	19	4	13	5	5	9	**151**
Germany	2	1			1		1		1			6	1		1	1	5	13	10	2	12	**57**
Italy	1	2	5	2	1		2		1		1	1	6	4	3	1	2	1	4	2	2	**41**
Canada					1				4	3	1		3			3	3	3	3	1	8	**33**
Japan	1	1	1	1						1					3	7	1					**16**
Total num. of attacks	46	54	27	39	11	21	15	9	30	8	17	19	25	29	21	50	34	51	33	30	75	644

Table 5. Number of terrorist attacks in the USA for each year, in the 2000-2020 period, for the specific ESIF macro-target

USA Targets/Year	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	Total
Airports & Aircraft			1							1				2		1		2		1		8
Business	19	22	4	22	3	5	2		2	2	5	1	2	2		7	7	8	5	10	6	134
Food or Water Supply																						
Journalists & Media		5									1						1	1	1			9
Maritime																						
Telecommunication										1										2	4	7
Transportation									1		1	1					1	2				6
Utilities									1				1	1	1		4				1	9
Total	19	27	5	22	3	5	2		4	4	7	2	3	5	1	8	13	13	6	13	11	173

Table 6. Number of terrorist attacks on the UK for each year, in the 2000-2020 period, for specific ESIF macro-target

UK Targets/Year	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	Total
Airports & Aircraft		1						1			1									2		5
Business	8	13	1	1	1	1	3	4	10		3	7		10	8	9	5	7	3	2	3	99
Food or Water Supply																						
Journalists & Media		2											1							2		5
Maritime																						
Telecommunication													1	1							30	32
Transportation	4	4				8		2	1		2		1		1	1	1	1	2	1		29
Utilities											1			1		1						3
Total	12	20	1	1	1	9	3	7	11		7	7	3	12	9	11	6	8	5	7	33	173

Table 7. Number of terrorist attacks on France for each year, in the 2000-2020 period, for specific ESIF macro-target

France Targets/Year	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	Total
Airports & Aircraft		1					1															2
Business	11	1	15	11	4	7	6	2	8		1	2	9	6	2	17	4	8	5	3	3	125
Food or Water Supply																						
Journalists & Media		1										1		2		1				1	2	8
Maritime																						
Telecommunication				1											2			2		1	3	9
Transportation									1							1		1			1	4
Utilities				1														2				3
Total	11	3	15	13	4	7	7	2	9		1	3	9	8	4	19	4	13	5	5	9	151

Table 8. Number of terrorist attacks on Italy for each year, in the 2000-2020 period, for specific ESIF macro-target

Italy Targets/Year	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	Total
Airports & Aircraft			1	1																		2
Business		1	1	1	1		1		1			1	6	1	1		2	1	2		1	21
Food or Water Supply																						
Journalists & Media	1	1	2				1							3					1	1		10
Maritime																						
Telecommunication																					1	1
Transportation			1								1				2	1			1	1		7
Utilities																						
Total	1	2	5	2	1		2		1		1	1	6	4	3	1	2	1	4	2	2	41

In Table 7, for the case of France, the data relating to attacks on "Business" targets in the entire 2000-2020 period is noteworthy, with 125 attacks out of a total of 151 recorded events.

In Table 8, for the case of Italy, the total number of attacks relating to "Journalists & Media" assets appears to be highlighted compared to the overall number of events (around a quarter of the events, e.g. 10 attacks out of a total of 41 events recorded in the 2000-2020 period).

5. THE CBREI THREAT

Maintaining the analysis period from 2000 to 2020, as an application of the data from the GTD database, the study firstly focused on the use of CBREI (Chemical, Biological, Radiological, Explosive, Incendiary) weapons worldwide.

The worldwide analysis considered the 12 macro-regions (indicated in the GTD with the variable Region) reported in the first column of Table 9.

This table shows how in the 21 years considered there were 81,425 CBREI attacks on all types of targets worldwide, with a very clear prevalence among these of type E (Explosive) and type I (Incendiary) attacks. In fact, type E attacks represent 90.8% of the overall attacks recorded for the CBREI, while type I attacks reach 8.87% of the overall value.

Table 9. Number of CBREI worldwide attacks recorded in the 12 macro-regions of the GTD (2000-2020 period)

Region	Total CBREI Attacks (2000-2020)	C	B	R	E	I
Middle East & North Africa	33,581	71	2		32,682	826
South Asia	26,391	81	2		24,183	2,125
Sub-Saharan Africa	6,890	10	3		5831	1,046
Southeast Asia	5,518	8			4,737	773
Western Europe	3,256	15			1,838	1,403
Eastern Europe	2,755	11			2,556	188
South America	1,955	9	1		1,649	296
North America	608	15	20		174	399
East Asia	187	5		10	115	57
Central Asia	140				124	16
Australasia & Oceania	93	8			7	78
Central America & Caribbean	51				34	17
Total	81,425	233	28	10	73,930	7,224

Table 10. Percentage values of the types of weapons used within the worldwide CBREI (2000-2020 period)

Weapon	Num. Attacks (2000-2020)	%
C	233	0.29
B	28	0.03
R	10	0.01
E	73,930	90.80
I	7,224	8.87
Total	81,425	100

These results expressed in percentages, shown in Table 10, highlight how - however relevant and present – the worldwide CBR type attacks are significantly lower in number, with 0.29% for the C (Chemical) case, 0.03% of the B (Biological) and 0.01% of the R (Radiological) case in the same 2000-2020 time gap.

Returning to the analysis of ESIF-type objectives within the G7 countries, the Table 11 shows the results obtained for CBREI attacks, for each individual country and for the same period 2000-2020.

Table 11. Number of CBREI attacks on ESIF targets and their distribution for G7 countries (2000-2020 period)

Nation	Total CBREI Attacks to ESIF	C	B	R	E	I
USA	129	2	7		20	100
UK	154				69	85
France	129				94	35
Germany	47				16	31
Italy	36				25	11
Canada	25				13	12
Japan	14				5	9
Total	534	2	7	0	242	283

In this case, the recorded attacks are 534 in total, with the record of 154 attacks related to the United Kingdom, followed by the USA and France (both with 129 CBREI attacks on ESIF targets).

The numbers obtained from the GTD show how type I and E attacks are absolutely significant in percentage terms, with 53% for case I and 45.32% for case E.

CBR attack types are very limited for the case of the G7 countries, with 7 type B attacks, 2 type C and no type R attacks in the period considered.

With reference to Table 12, the analysis focuses - again for the case of CBREI weapons for the G7 countries in the 2000-2020 period - on the individual ESIF TargetTypes, e. g. on the 8 targets reported in the first column of the table.

As already highlighted in the previous cases, the main objective targeted by terrorists appears to be - in this context - "Business" followed by "Transportation" and "Telecommunication".

Table 12. Number of CBREI attacks on individual ESIF targets and their breakdown by G7 countries (2000-2020 period)

ESIF Target Types	Total CBREI Attacks to SEIF for G7 Nations	C	B	R	E	I
Airports & Aircraft	13				11	2
Business	353	2	2		167	182
Food or Water Supply	1				1	
Journalists & Media	23		5		11	7
Maritime	0					
Telecommunication	56				1	55
Transportation	66				39	27
Utilities	22				12	10
Total	534	2	7	0	242	283

The Table 13 shows, as an example, the analysis of terrorist attacks on ESIF targets in Italy using CBREI weapons for the 2000-2020 period.

As shown in Table 13, there are only cases of type E (Explosives) and I (Incediary) attacks, with a marked prevalence of 'Business' objectives (in total, 16 attacks out of a total of 36 terrorist events).

In particular, as an example of the TargetSubType level for Italy, the following Table 14 shows the maximum detail (in terms of sub-types of objectives) that can be identified in the GTD.

The table highlights how the two most affected SubTypes in the observation period were the specific targets "Newspaper Journalist/Staff/Facility" with 6 type E attacks and "Train/Train Tracks/Trolley" with 5 type I attacks.

It is also highlighted that in 2016 and 2018, type E attacks on "Bank/Commerce" facilities (in the TargetType "Business") occurred in Italy, for a total of 2 attacks of this type in the complete 2000-2020 period.

Finally, it is highlighted that in Italy, in the period 2000-2020, no CBR-type attack on ESIF targets was recorded.

Table 13. Number of attacks on ESIF targets in Italy per year with CBREI weapons (2000-2020 period)

Italy	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	Total
Explosives	**1**	**2**	**4**	**2**	**1**		**2**				**1**	**1**	**4**	**2**	**1**		**1**	**1**	**1**		**1**	**25**
Airports & Aircraft			1	1																		2
Business		1	1	1	1		1					1	4	1	1		1	1	1		1	16
Journalists & Media	1	1	2				1							1								6
Transportation											1											1
Incendiary			**1**										**1**		**2**	**1**	**1**		**2**	**2**	**1**	**11**
Business													1				1		1			3
Journalists & Media																				1		1
Telecommunication																					1	1
Transportation			1												2	1			1	1		6
Total	1	2	5	2	1		2				1	1	5	2	3	1	2	1	3	2	2	36

Table 14. Number of attacks on ESIF targets per year for Italy with CBREI weapons, up to the analysis level of TargetSubType (2000-2020 period)

Italy	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	Total
Explosives (total)	**1**	**2**	**4**	**2**	**1**		**2**				**1**	**1**	**4**	**2**	**1**		**1**	**1**	**1**		**1**	**25**
***Airports & Aircraft* (*subtotal*)**			**1**	**1**																		**2**
Airline Officer/Personnel				1																		1
Airport			1																			1
***Business* (*subtotal*)**		**1**	**1**	**1**	**1**		**1**					**1**	**4**	**1**	**1**		**1**	**1**	**1**		**1**	**16**
Bank/Commerce																	1		1			2
Construction							1							1	1							3
Entertainment/Cultural/ Stadium/Casino			1																			1
Industrial/Textiles/Factory												1										1
Legal Services																					1	1
Multinational Corporation				1	1																	2
Retail/Grocery/Bakery													1					1				2
(vuoto)		1											3									4
***Journalists & Media* (*subtotal*)**	**1**	**1**	**2**				**1**							**1**								**6**
Newspaper Journalist/Staff/Facility	1	1	2				1							1								6
***Transportation* (*subtotal*)**											**1**											**1**
Train/Train Tracks/Trolley											1											1
Incendiary (total)			**1**										**1**		**2**	**1**	**1**		**2**	**2**	**1**	**11**
***Business* (*subtotal*)**													**1**				**1**		**1**			**3**
Gas/Oil/Electric																	1					1
Retail/Grocery/Bakery																			1			1
(vuoto)													1									1
***Journalists & Media* (*subtotal*)**																				**1**		**1**
Newspaper Journalist/Staff/Facility																				1		1
***Telecommunication* (*subtotal*)**																					**1**	**1**
Telephone/Telegraph																					1	1
***Transportation* (*subtotal*)**			**1**												**2**	**1**			**1**	**1**		**6**
Subway			1																			1
Train/Train Tracks/Trolley															2	1			1	1		5
Total		1	2	5	2	1		2				1	1	5	2	3	1	2	1	3	2	2	36

6. MITIGATION OF RISKS FROM ACTIONS OF SABOTAGE AND TERRORISM IN ITALY

The in-depth study of the historical events related to terrorism actions on ESIF (Essential Services, Infrastructures and Facilities) objectives in the 2000-2020 timeframe and the analysis carried out as part of the 2022 Annual Italian Report on Information Policy for Security [19] (released by the Italian Intelligence Section in February 2023) were considered in order to evaluate the appropriateness and potential effectiveness of the 'Scudo Italia' protocol [20].

This protocol, presented in 2020 [20], constitutes an AS/AT (anti-sabotage/anti-terrorism) Security Risk Management tool applicable to industrial contexts and critical infrastructures (physical areas, operational processes and supply chains) of national strategic importance and promoted by the Italian Observatory for the Security of National Strategic Industrial System (O.S.S.I.S.Na.) with the aim of effectively implementing an organizational model of security management, operations continuity & crisis communication to be applied in the event of a 'state of emergency'.

The proposed organizational model is applied in so-called 'crisis scenarios', considered as unconventional situations in which external factors – of which the effects are not

adequately predictable - can cause serious damage to the operational capacity of the organization itself. Typical crisis scenarios are health or pandemic emergencies, war events, terrorist acts and socio-economic crises.

The Protocol is mainly aimed at mitigating risks deriving from threats of a physical, biological, cyber and financial nature from hostile national and foreign entities, with the aim of interdiction and sabotage of operational activities or malicious acquisition of technological capabilities.

Every possible hostile event for each of the threats considered is assessed in its impact and probability [20] of occurrence on the basis of the information acquired in cooperation with the national public security and intelligence agencies responsible for the purpose, arriving at the definition of the 'risk level' (according to categories: acceptable, medium, unacceptable). For each level of risk, the need for mitigation intervention is also established, which may involve organizational, operational, technological and financial options.

This Protocol was specifically applied in an ex-post simulation to some of the events reported in Table 14 in order to evaluate its potentiality and capabilities. The results of this simulation will be illustrated in a future paper.

As a matter of fact, the availability and sharing by the Intelligence Bodies towards the interested Economic Operators of detailed information about the threat scenarios could be a useful pre-condition, in order to be able to set the integrated security management, operations continuity & crisis communication plan in the most effective and efficient way possible, resulting in a significant improvement in terms of resilience of the organization itself.

7. CONCLUSIONS

Starting from the latest data made publicly available from one of the most important global terrorist attack databases, the Global Terrorism Database, maintained by the START consortium and Maryland University, a detailed analysis on the evolution over the last 21 years of terrorist attacks on specific targets related to critical infrastructure to essential services and strategic facilities was conducted for G7 countries.

Specifically, the results of developing a set of specific targets (TargetType) extracted from the GTD, referred to in the document as the ESIF (Essential Services, Infrastructures and Facilities) macro-target, with a focus on G7 countries, were presented. This macro-target typically contains most of a country's industrial assets, infrastructures and strategic services.

In particular, the analysis on the ESIF macro-target was conducted in a timely manner for the period 2000-2020 for the seven G7 countries, in order to carry out a comparison of the different situations recorded in the most developed world countries, intercept possible trends, also verifying the type of weapon used for the attack, focusing the analysis on CBREI attacks, which constitute the most destructive and impactful terrorist attacks found in the GTD.

Among the various results obtained, the analysis showed for CBREI attacks over the period 2000-2020 for G7 countries that type E attacks account for 90.8% of the total terrorist events for CBREI attacks, while type I attacks reach 8.87% of the total value, relegating the cumulative percentage of CBR attacks in G7 countries to the value of 0.33% over the 21 years considered in the analysis.

For the ESIF-Type objectives the results obtained for CBREI attacks in the G7 countries show a total number of 534 events in the period 2000-2020, with the top of the rank for the 154 attacks (28.8%) related to the United Kingdom, followed by the USA and France ones, both with 129 (24.2%) CBREI attacks on ESIF targets. Finally, the main objective targeted by terrorists for CBREI attacks in the G7 countries appears to be "Business" followed by "Transportation" and "Telecommunication".

The methodology defined with this study (definition of target categories and sub-categories, identification of the various types of events, extrapolation and processing of data, identification of time intervals) aims to specific situational updates in an efficient way, allowing comparable and organic periodic evaluations.

REFERENCES

[1] Papa, M., Shenoi, S. (2008). Critical Infrastructure Protection II. Spinger, ISBN 978-0-387-88522-3.

[2] Alcaraz, C., Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. International Journal of Critical Infrastructure Protection, 8: 53-66. http://dx.doi.org/10.1016/j.ijcip.2014.12.00

[3] Zoli, C., Steinberg, L.J., Grabowski, M., Hermann, M. (2018). Terrorist critical infrastructures, organizational capacity and security risk. Safety Science, 110: 121-130. http://dx.doi.org/10.1016/j.ssci.2018.05.021

[4] US NIAC, National Infrastructure Advisory Council (2008). Critical infrastructure partnership strategic assessment final report and recommendations. https://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf.

[5] US DHS, Department of Homeland Security (2013). National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience. https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

[6] US CISA (2024). Critical Infrastructure Sectors and Plans. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

[7] Directive (EU) 2008/114/EC. (2008). Identification and designation of European critical infrastructures and the assessment of the need to improve their protection. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114.

[8] Directive (EU) 2022/2555 of the European Parliament and of the Council. (2022). Measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555.

[9] Directive (EU) 2022/2557 of the European Parliament and of the Council. (2022). Resilience of critical entities and repealing, Council Directive 2008/114/EC. https://eur-lex.europa.eu/eli/dir/2022/2557/oj.

[10] Global Terrorism Database (GTD), START (National Consortium for the Study of Terrorism and Responses to Terrorism), University of Maryland. https://www.start.umd.edu/gtd/.

[11] Miller, E. (2016). Terrorist attacks targeting critical infrastructure in the United States, 1970-2015. Report to the U.S. Department of Homeland Security. https://www.start.umd.edu/pubs/DHS_I&A_GTD_Targeting%20Critical%20Infrastructure%20in%20the%20US_June2016.pdf.

[12] Global Terrorism Database codebook: Methodology, inclusion criteria, and variables. (2022). START (National Consortium for the Study of Terrorism and Responses to Terrorism), (2021, August). University of Maryland. https://www.start.umd.edu/gtd/downloads/Codebook.pdf.

[13] Li, Z., Li, X., Dong, C., Guo, F., Zhang, F., Zhang, Q. (2021). Quantitative analysis of global terrorist attacks based on the global terrorism database. Sustainability, 13(14): 7598. https://doi.org/10.3390/su13147598

[14] Hu, X., Lai, F., Chen, G., Zou, R., Feng, Q. (2019). Quantitative research on global terrorist attacks and terrorist attack classification. Sustainability, 11(5): 1487. https://doi.org/10.3390/su11051487

[15] Carbonelli, M. (2019). Terrorist attacks and natural/anthropic disasters: Risk analysis methodologies for supporting security decision making actors. Aracne CBRN Series, Rome.

[16] Carbonelli, M., Iannotti, A., Malizia, A. (2021). Disaster management of a major CBRN accident. In A. J. Masys (ed.), Handbook of Security Science, Springer Nature Switzerland AG 2020. http://doi.org/10.1007/978-3-319-51761-2_36-1

[17] Carbonelli, M. (2023). Attacks against Buildings: Threats, Vulnerabilities and Risk Assessment. CISINT Rome. ISBN: 979-12-210-4808-7, https://www.cisint.org/cms/wp-content/uploads/Attacks-against-buildings-M.Carbonelli-CISINT-2023.pdf.

[18] Gaub, F. (2017). Trends in terrorism, European Union Institute for Security Studies (EUISS), https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_4_Terrorism_in_Europe_0.pdf.

[19] Annual Report 2022 of Italian Intelligence, Relazione Annuale 2022 sulla Politica dell'Informazione per la Sicurezza - Presidenza del Consiglio dei Ministri. https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2023/02/Relazione_annuale_2022_interattiva.pdf.

[20] Sesler, F., Iavarone, V., Todaro, C., Petrini, K., Di Traglia, S. (2020). Observatory for the security of national strategic industrial system. International Conference SICC2020, Rome (Italy). https://www.cisint.org/cms/wp-content/uploads/SICC2020_OSSISNA_presentantion_09122020_ENG.pdf.

NOMENCLATURE

AS	AntiSabotage
AT	AntiTerrorism
CBR	Chemical, Biological, Radiological
CBREI	Chemical, Biological, Radiological, Explosive, Incendiary
CER	Critical Entities Resilience
ESIF	Essential Services, Infrastructures and Facilities
EU	European Union
G7	Group of 7 (USA, UK, France, Germany, Italy, Canada and Japan)
GTD	Global Terrorist Database
NIS	Network and Information Security
O.S.S.I.S.Na.	Italian Observatory for the Security of National Strategic Industrial System
START	Study of Terrorism and Responses to Terrorism
TT	TargetType