Gli attacchi alle IC del settore E&U

Le dimensioni del fenomeno, i motivi degli attacchi
e analisi di casi studio significativi

Workshop IBM settore E&U
Milano, 21 settembre 2011

Marco Dugato e Michele Riccardi
TRANSCRIME – Joint Research Centre on Transnational Crime (Università Cattolica del Sacro Cuore / Università degli studi di Trento)

Programma dell'intervento

1. **Le dimensioni del fenomeno:**

   Quanto sono frequenti e diffusi gli attacchi alle infrastrutture critiche (IC) del settore E&U?

2 **Le criticità del fenomeno:**

   Cosa rende una IC del settore E&U problematica e vulnerabile?

3. **Prevenzione e security: spunti di riflessione**

   Riflessione sui moventi degli attacchi alle IC nel settore E&U e sui nuovi rischi per la security

1. Le dimensioni del fenomeno

Quanto sono frequenti e diffusi gli attacchi alle infrastrutture critiche (IC) nel settore E&U?

Definizione operativa IC adottata nell'analisi

- ✓ Ogni impianto, pubblico o privato, che fornisce servizi di utilità pubblica come la conduzione di acqua, l'evacuazione delle acque reflue, l'energia, il combustibile o le comunicazioni (Nazioni Unite, Convenzione del 23 dicembre 2002)

- ✓ Beni, sistemi o parti di essi che sono essenziali per il mantenimento delle funzioni sociali vitali, della salute, della sicurezza (*security* e *safety*), del benessere economico e sociale della popolazione, e la cui distruzione o il cui malfunzionamento avrebbe come diretta conseguenza un impatto significativo come risultato del mancato svolgimento di queste funzioni (*loss of service*) (Commissione Europea, Direttiva [EU4], 2008).

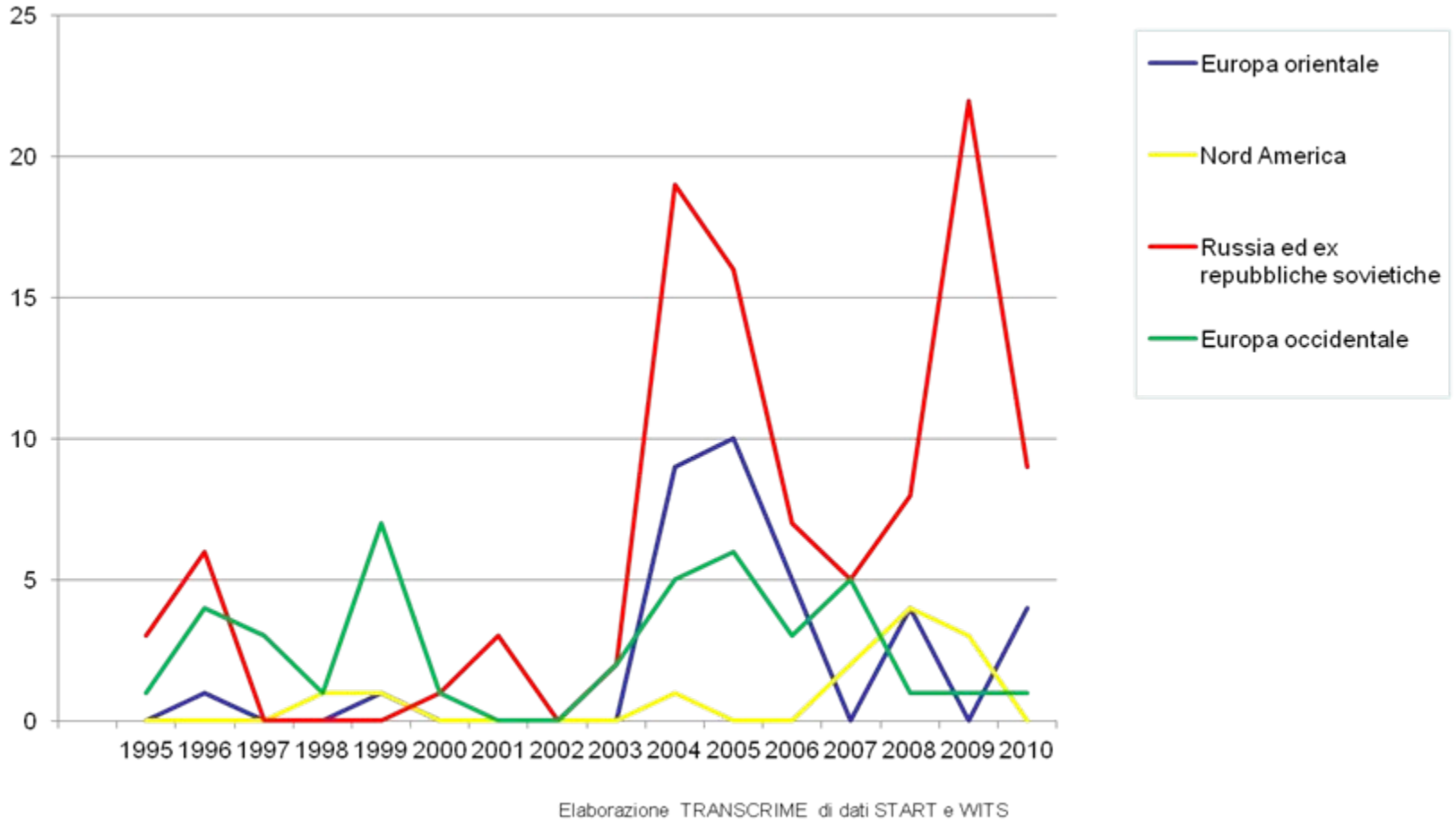
Gli attacchi alle IC E&U – 1995-2010

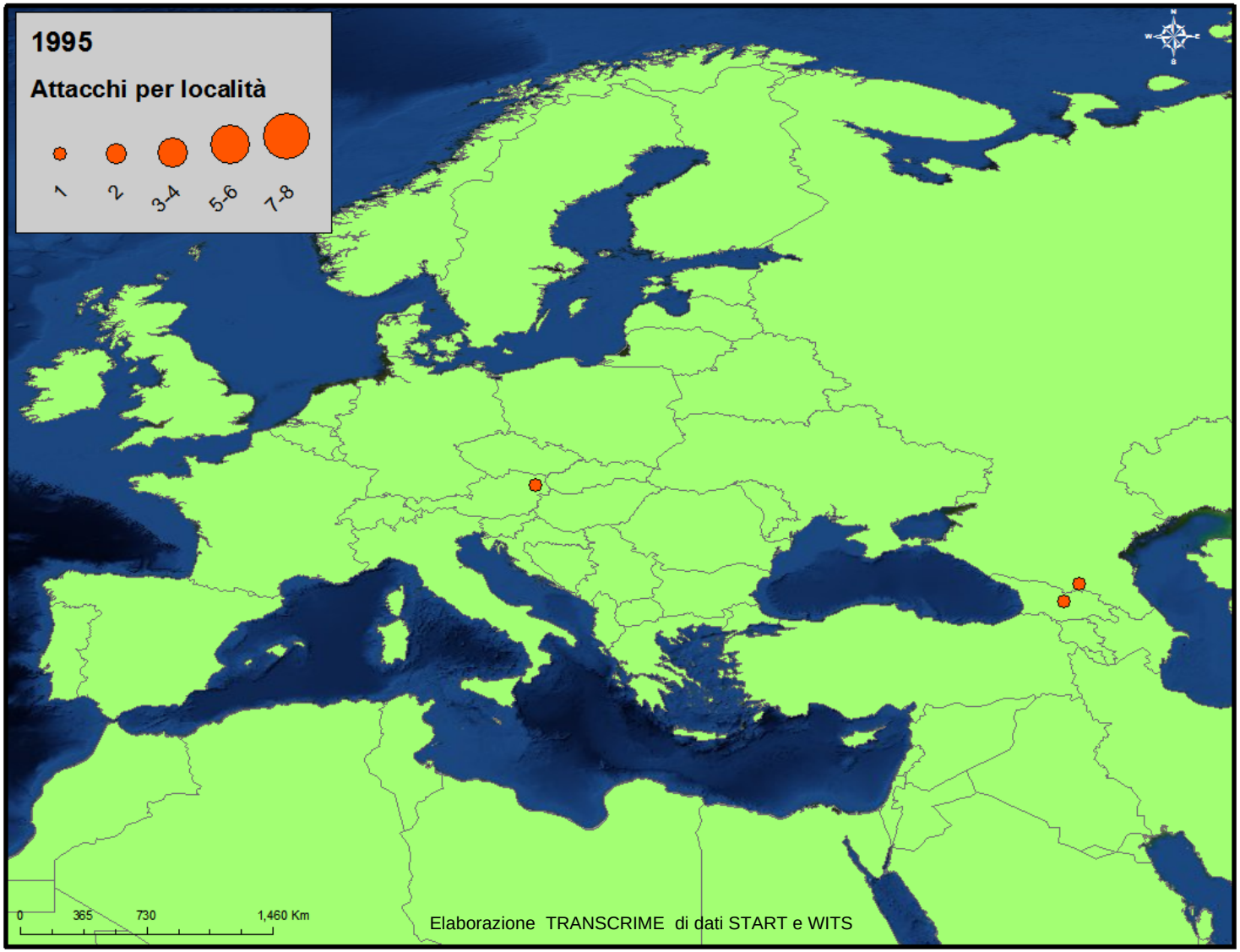
- ✓ **Fonte:** Elaborazione Transcrime su dati START (US Dept Homeland Security), WITS (FBI) e fonti aperte (stampa locale ed internazionale, internet).
- ✓ **Periodo:** Dal 1995 al 2010
- ✓ **Regioni analizzate:** Europa E & W, Russia ed ex membri URSS, N America

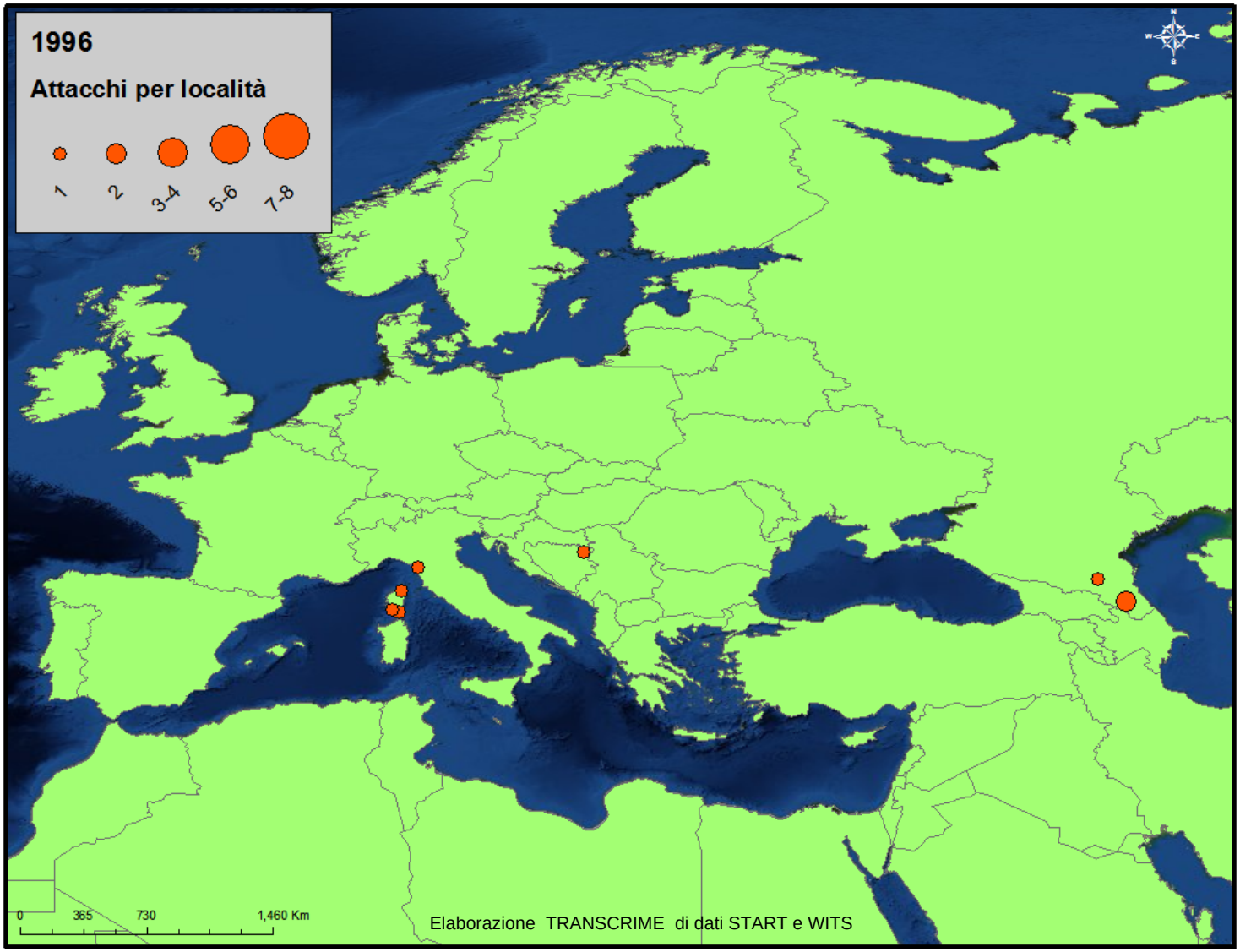
Key Figures:

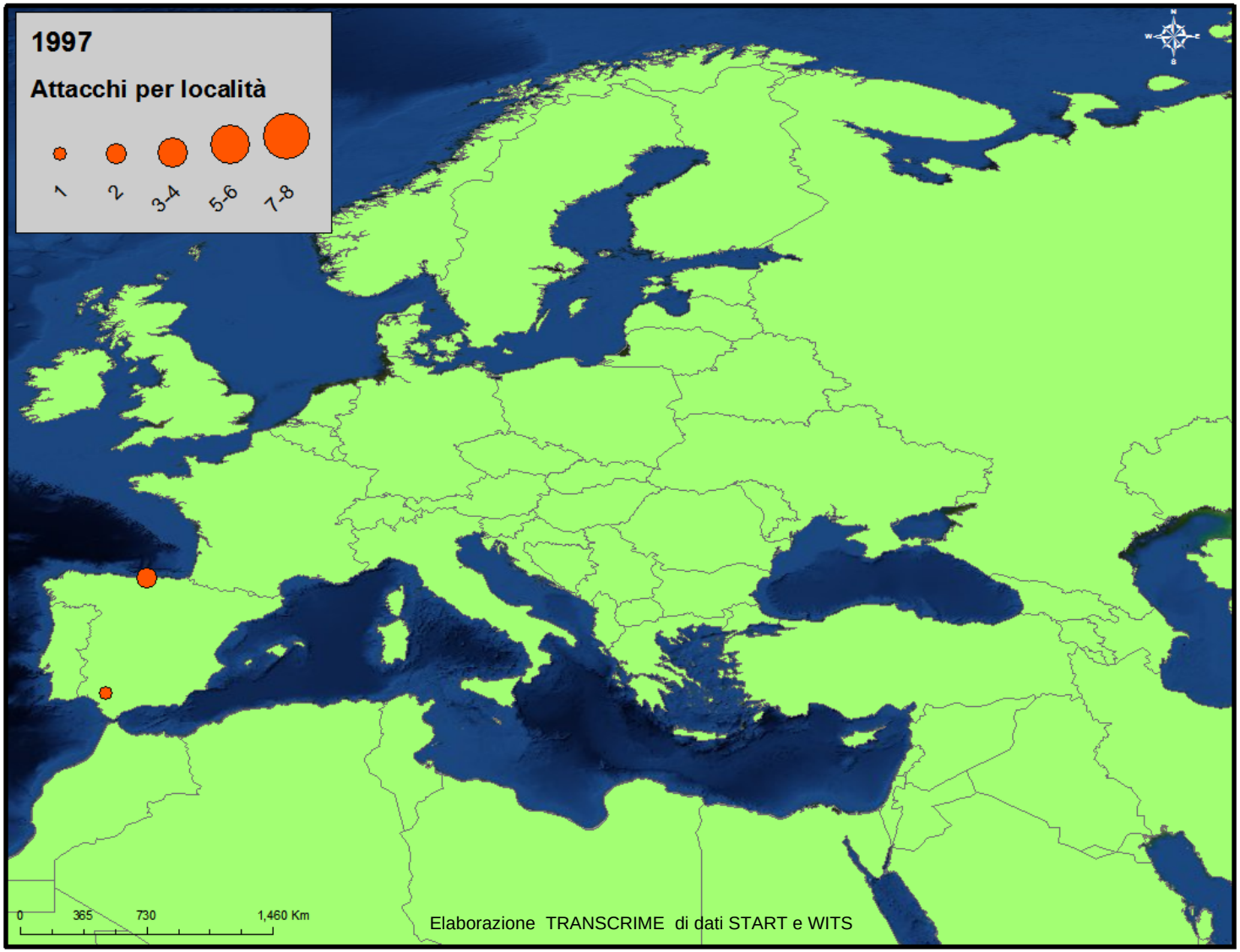
- ✓ **189 attacchi** totali
- ✓ In Europa E&W e America N attacchi concentrati in **zone specifiche** (Corsica, Quebec, Paesi Baschi)
- ✓ In ex URSS **crescita esponenziale** degli attacchi da metà anni 2000
- ✓ In Europa E&W e America N movente principalmente **politico/sociale o sconosciuto**
- ✓ In ex URSS in un terzo dei casi movente **etnico-religioso**
- ✓ In Europa E&W attacchi principalmente a **infrastrutture rete elettrica/centrali**
- ✓ In ex URSS attacchi principalmente a **Oil & Gas**

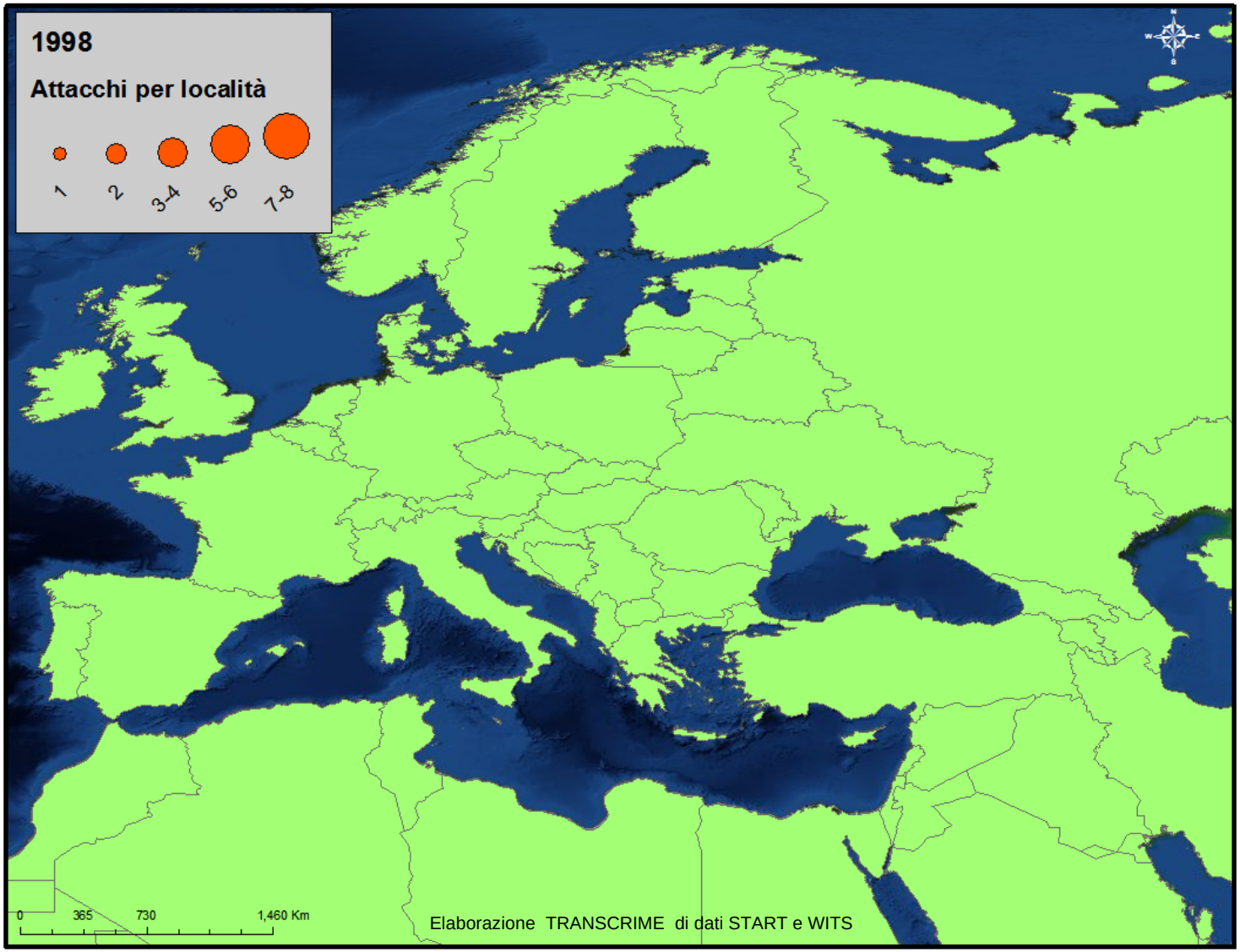
Attacchi verso IC E&U – 1995-2010

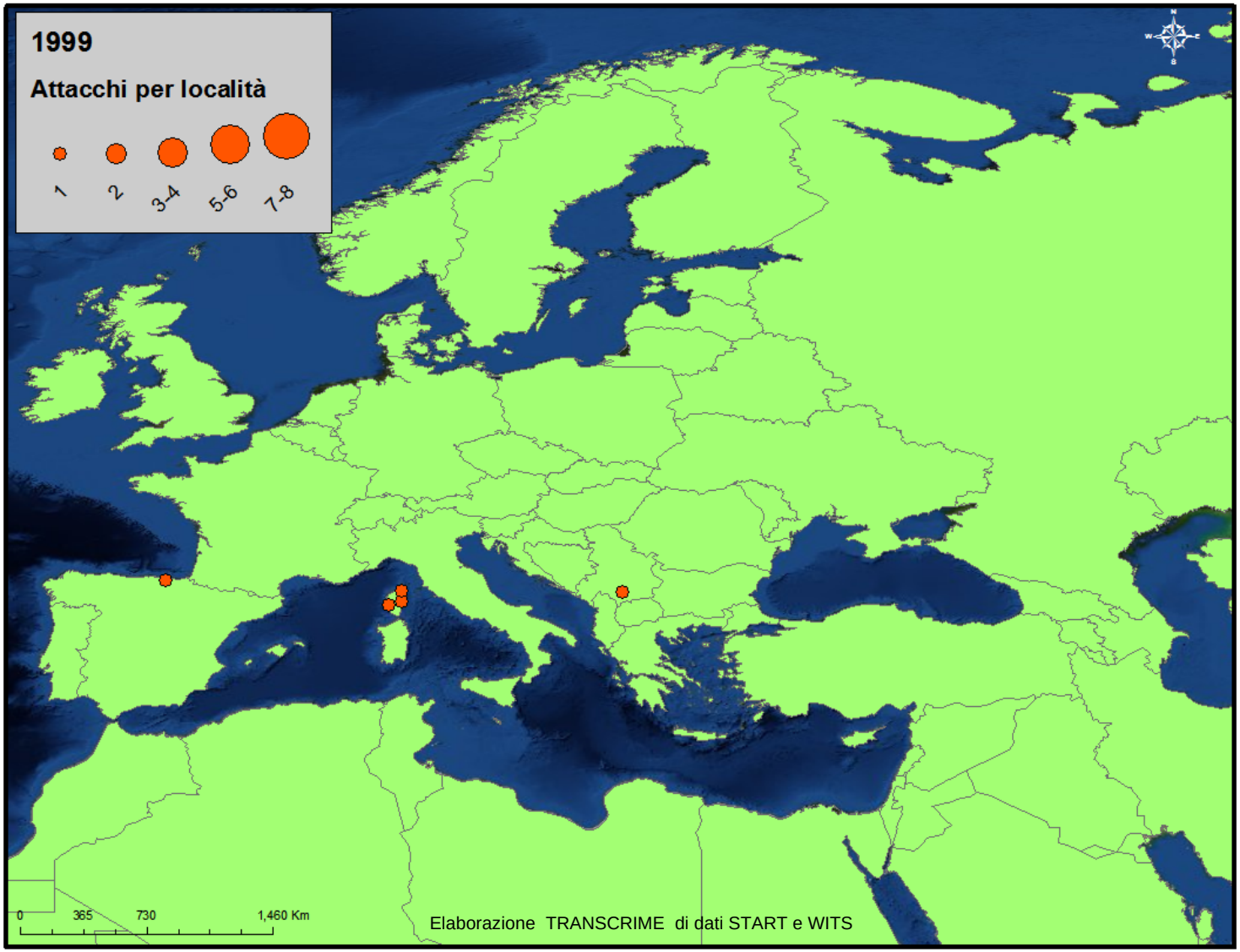


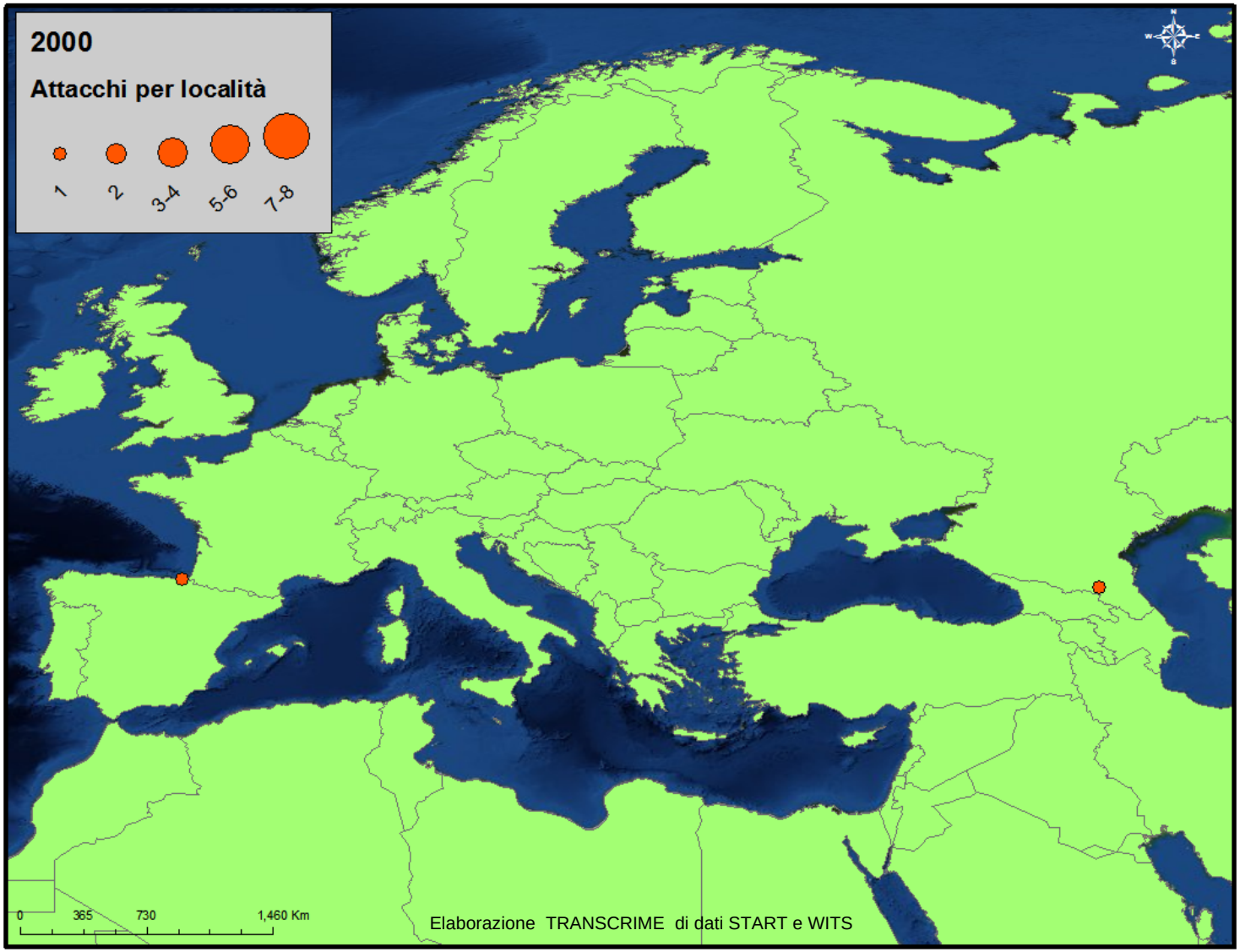

1995
Attacchi per località
1
2
3-4
5-6
7-8
0
365
730
1,460 Km
Elaborazione TRANSCRIME di dati START e WITS

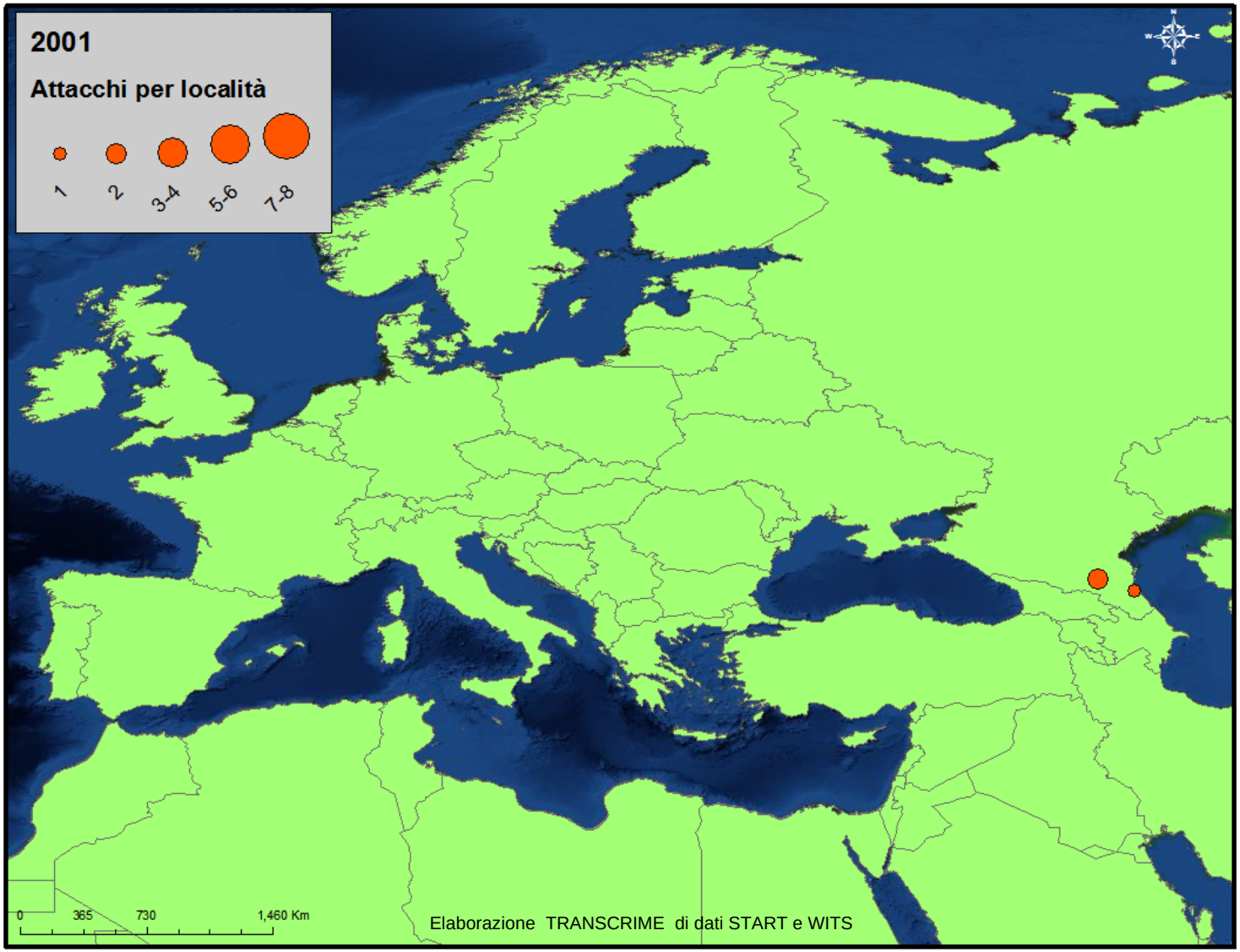

1996
Attacchi per località
1
2
3-4
5-6
7-8
0
365
730
1,460 Km
Elaborazione TRANSCRIME di dati START e WITS

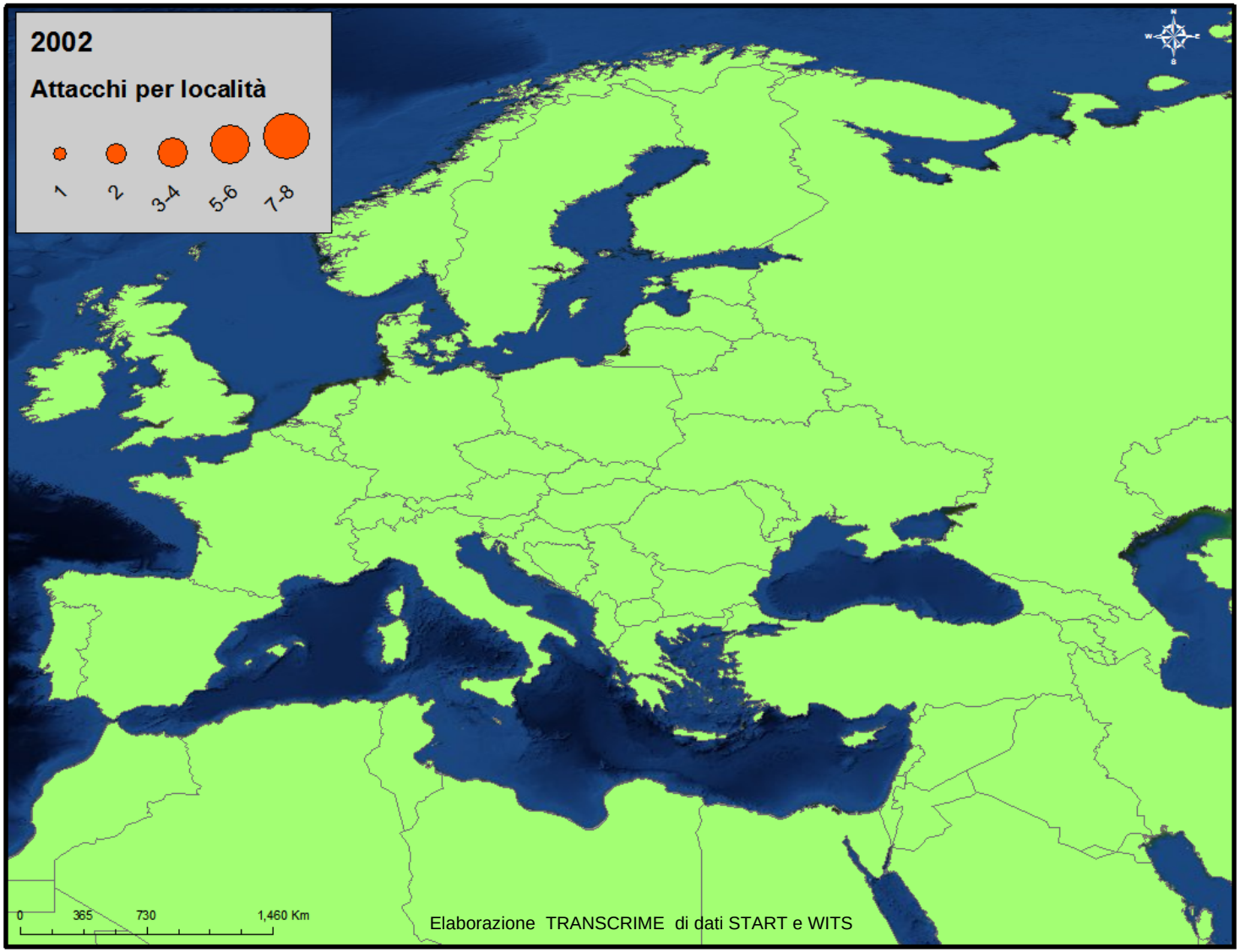

1997
Attacchi per località
1
2
3-4
5-6
7-8
0
365
730
1,460 Km
Elaborazione TRANSCRIME di dati START e WITS

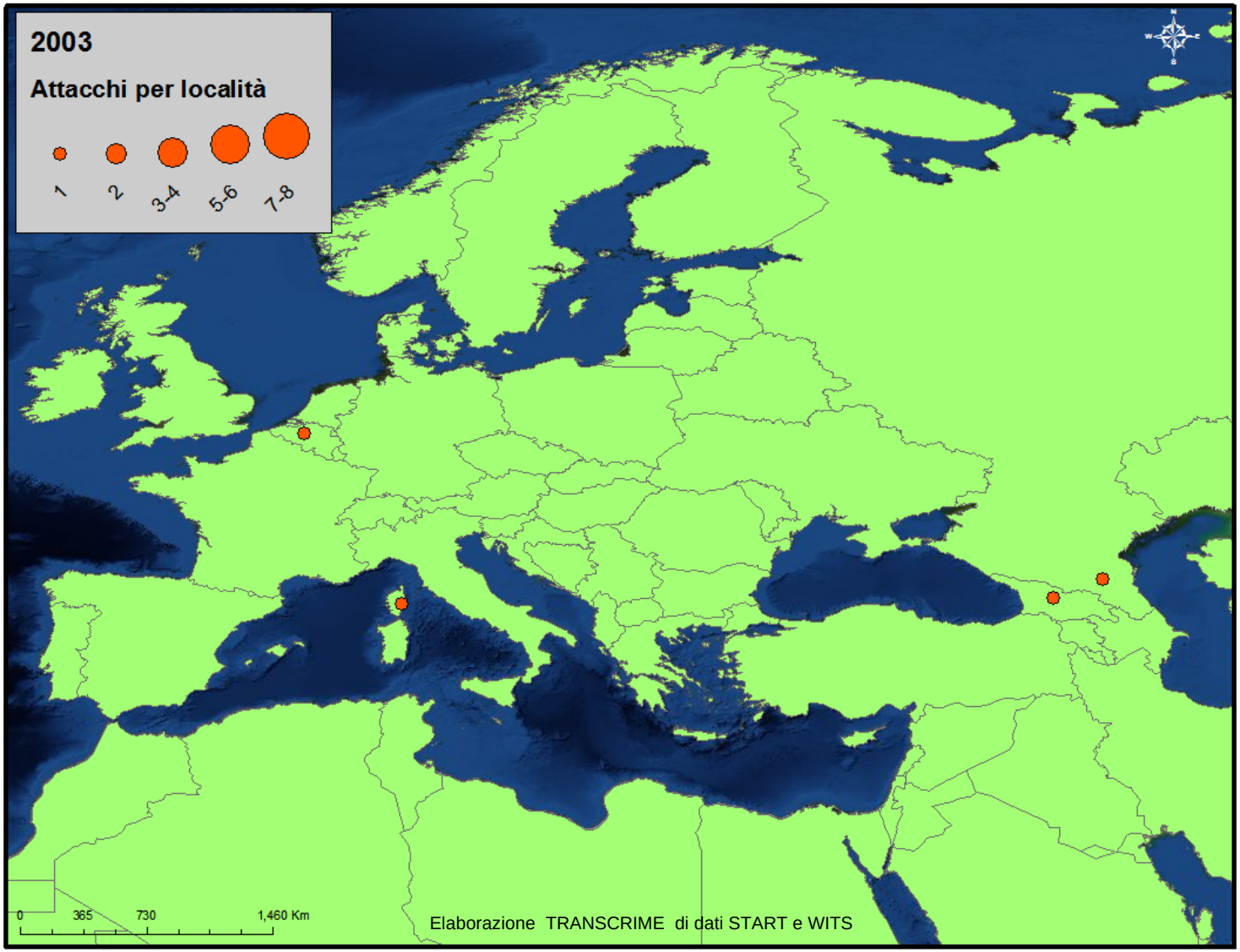

1998
Attacchi per località
1
2
3-4
5-6
7-8
0
365
730
1,460 Km
Elaborazione TRANSCRIME di dati START e WITS

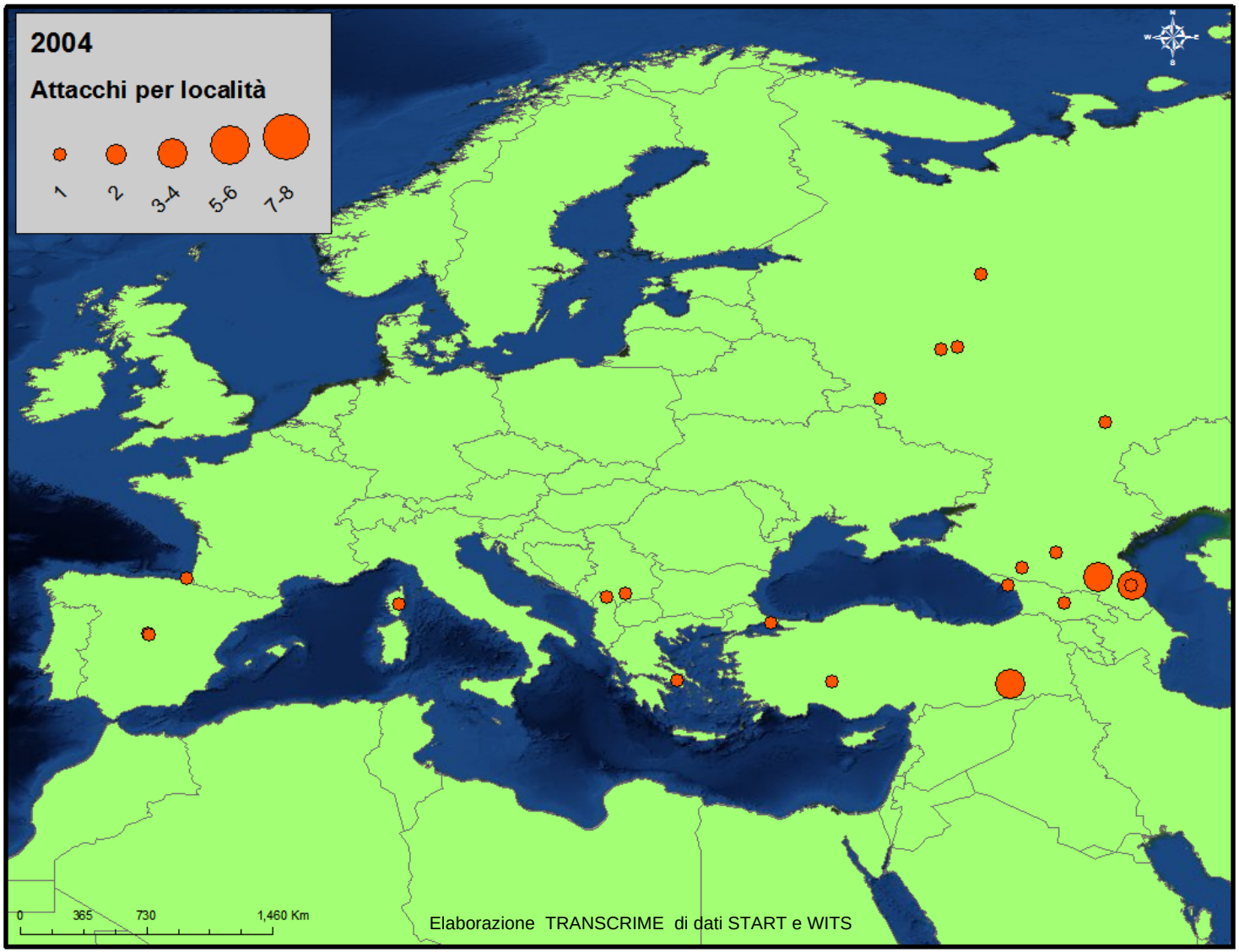

1999
Attacchi per località
1
2
3-4
5-6
7-8
0
365
730
1,460 Km
Elaborazione TRANSCRIME di dati START e WITS

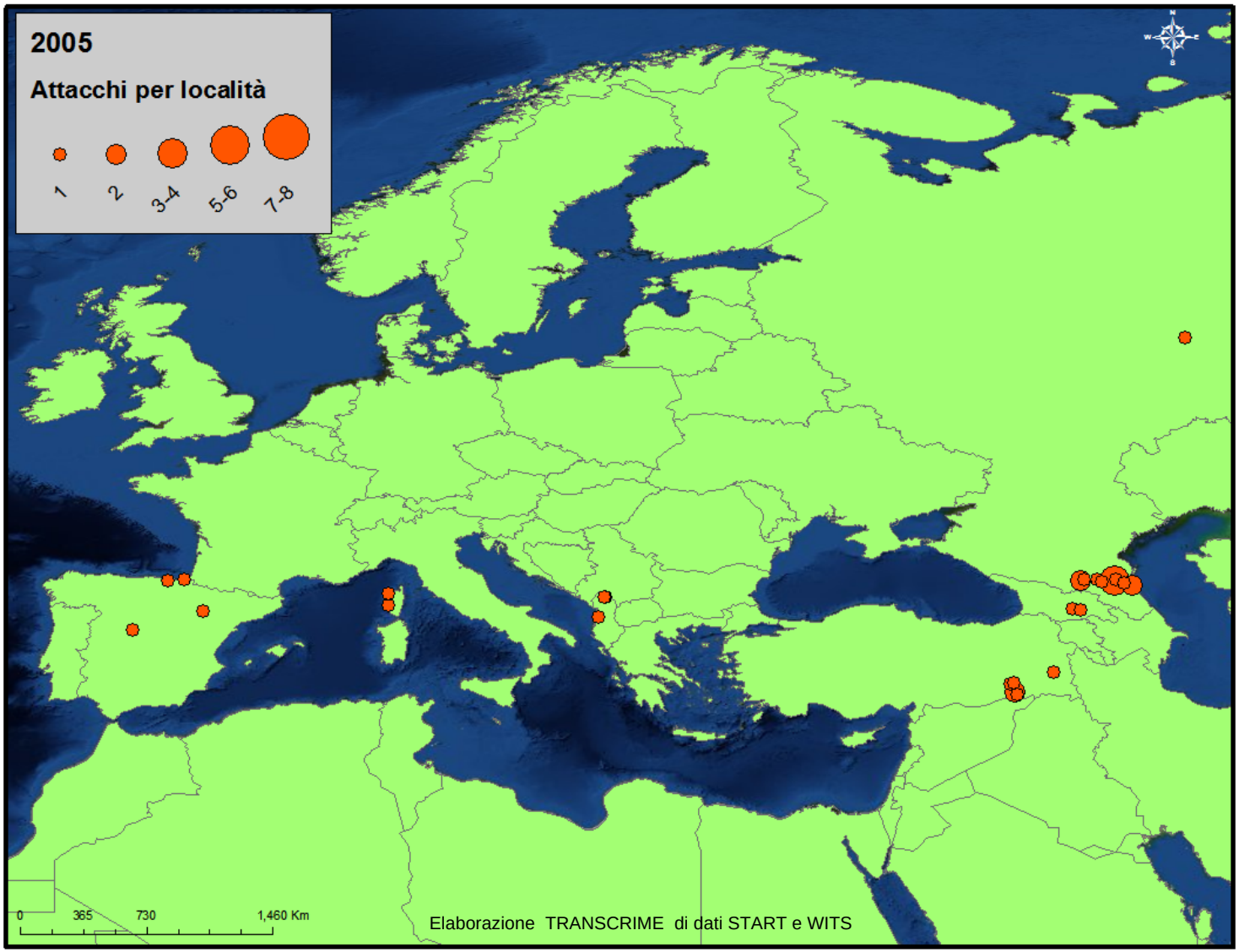

2000
Attacchi per località
1
2
3-4
5-6
7-8
0
365
730
1,460 Km
Elaborazione TRANSCRIME di dati START e WITS

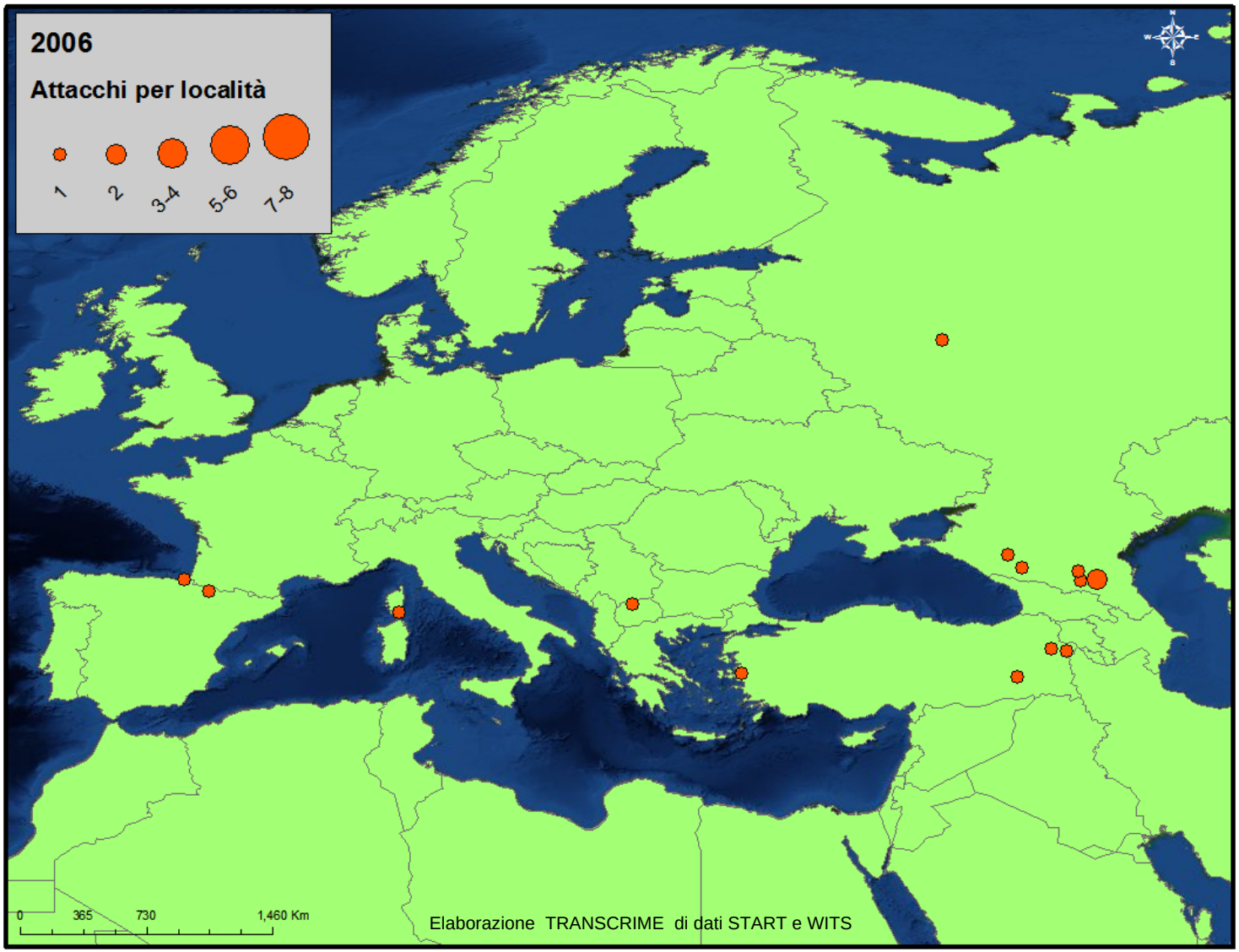

2001
Attacchi per località
1
2
3-4
5-6
7-8
0
365
730
1,460 Km
Elaborazione TRANSCRIME di dati START e WITS

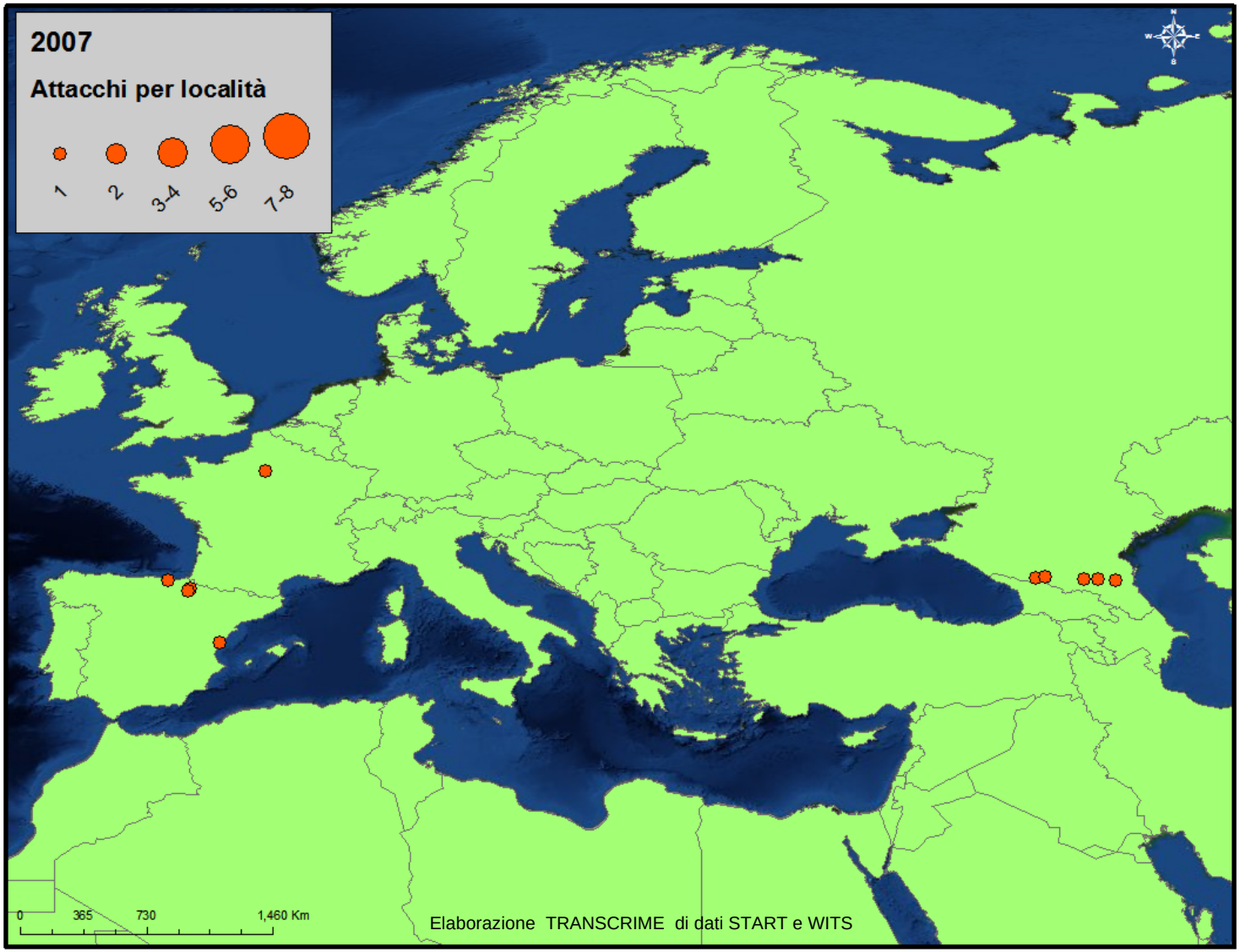

2002
Attacchi per località
1
2
3-4
5-6
7-8
0
365
730
1,460 Km
Elaborazione TRANSCRIME di dati START e WITS

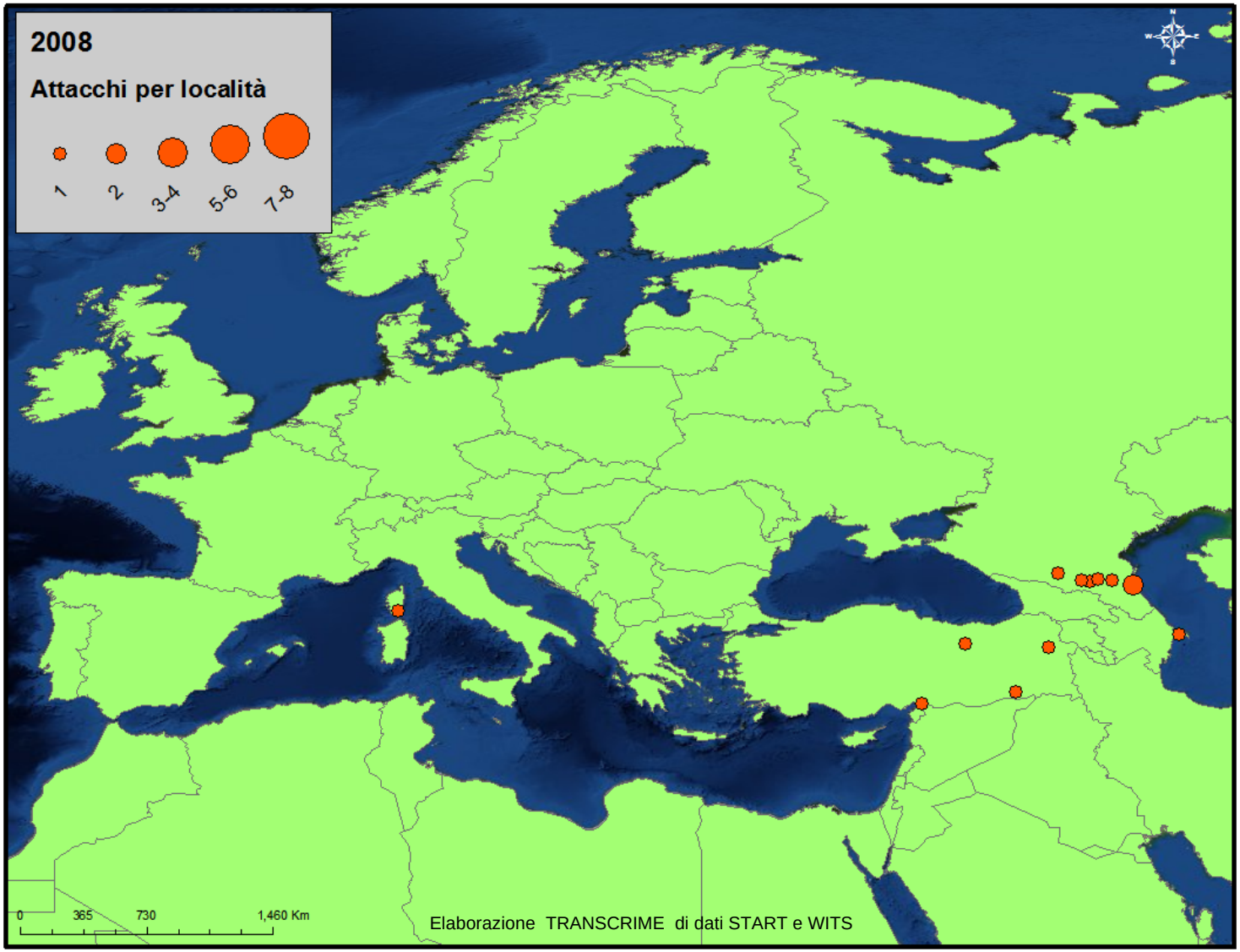

2003
Attacchi per località
1
2
3-4
5-6
7-8
0
365
730
1,460 Km
Elaborazione TRANSCRIME di dati START e WITS

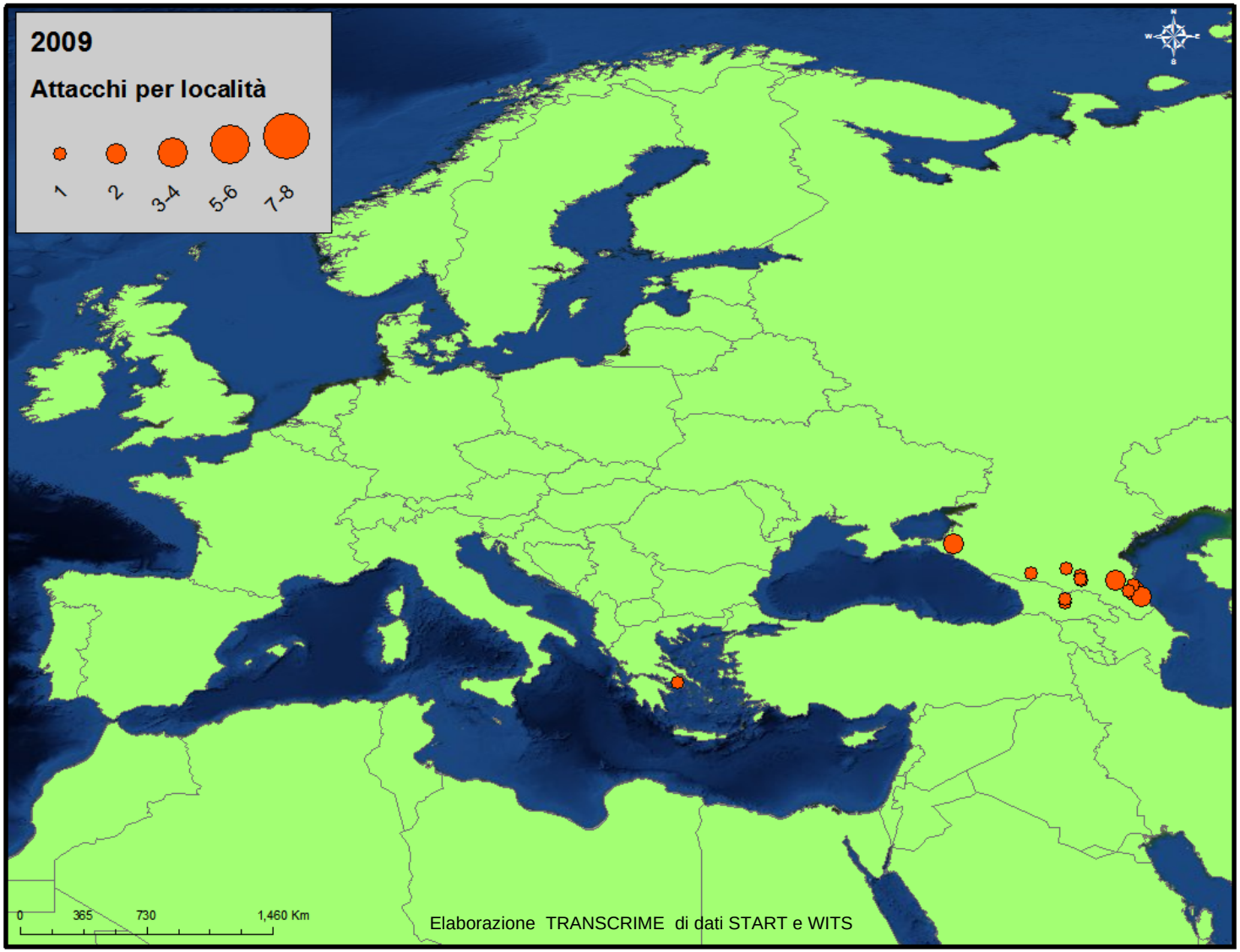

2004
Attacchi per località
1
2
3-4
5-6
7-8
0
365
730
1,460 Km
Elaborazione TRANSCRIME di dati START e WITS

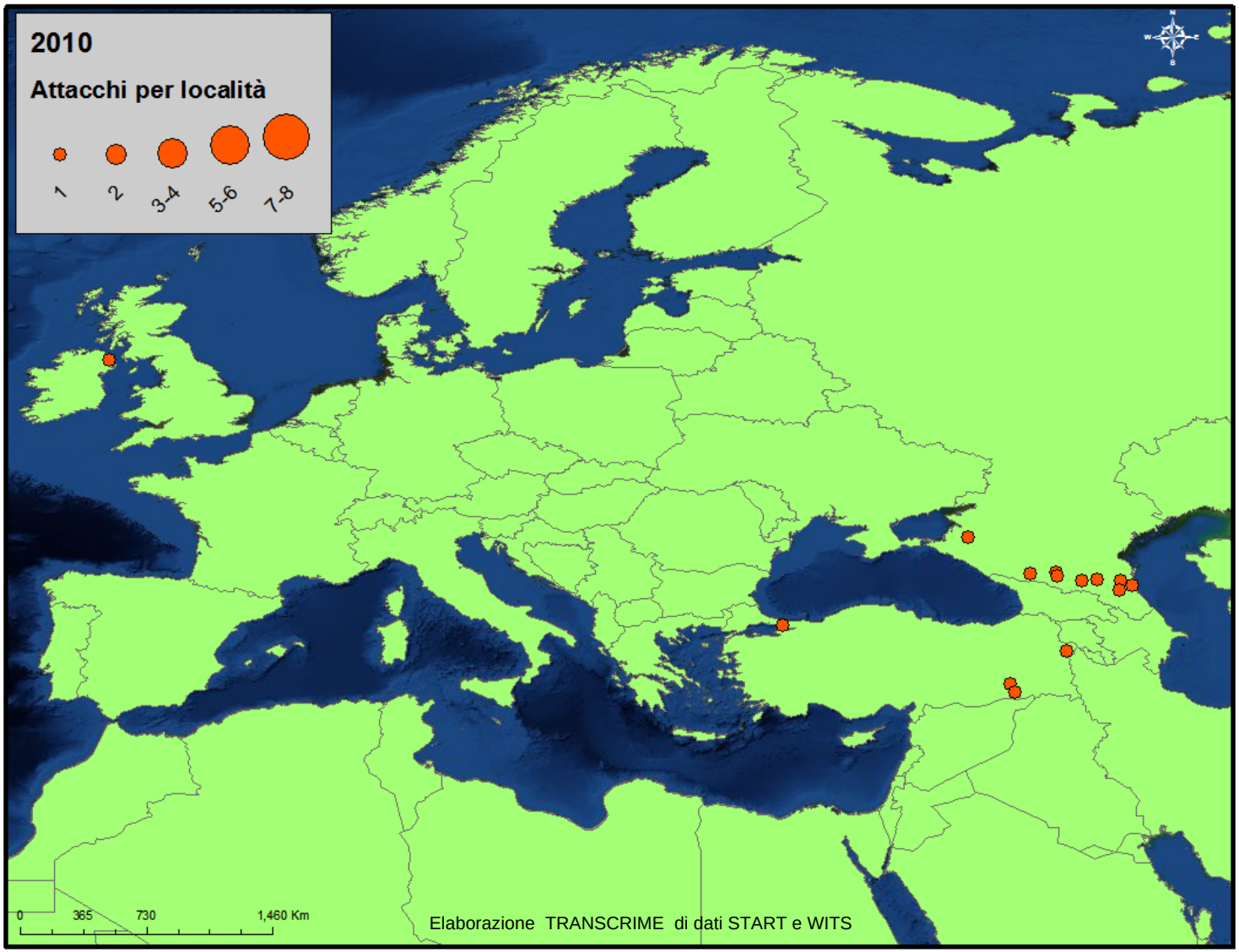

2005
Attacchi per località
1
2
3-4
5-6
7-8
0
365
730
1,460 Km
Elaborazione TRANSCRIME di dati START e WITS

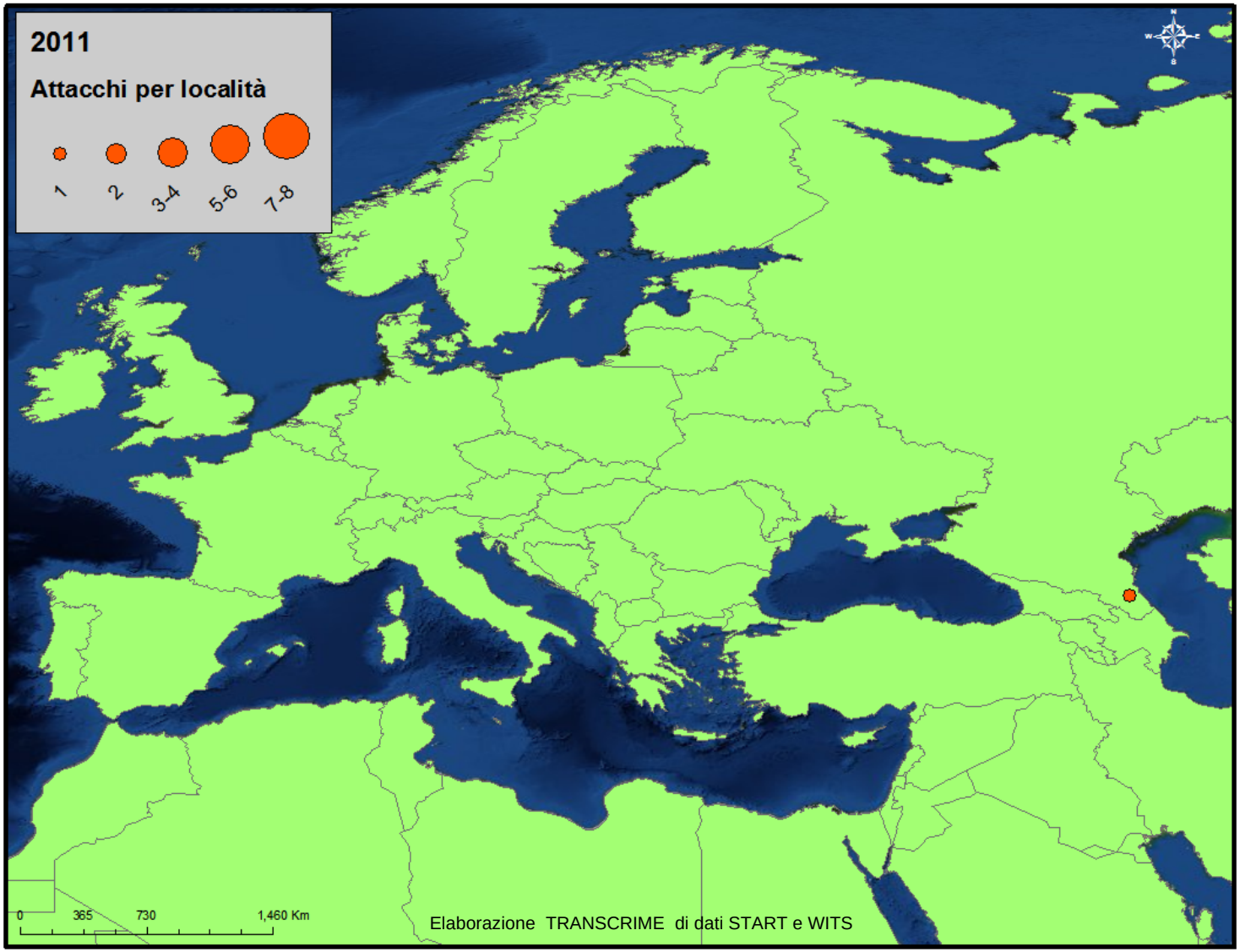

2006
Attacchi per località
1
2
3-4
5-6
7-8
0
365
730
1,460 Km
Elaborazione TRANSCRIME di dati START e WITS

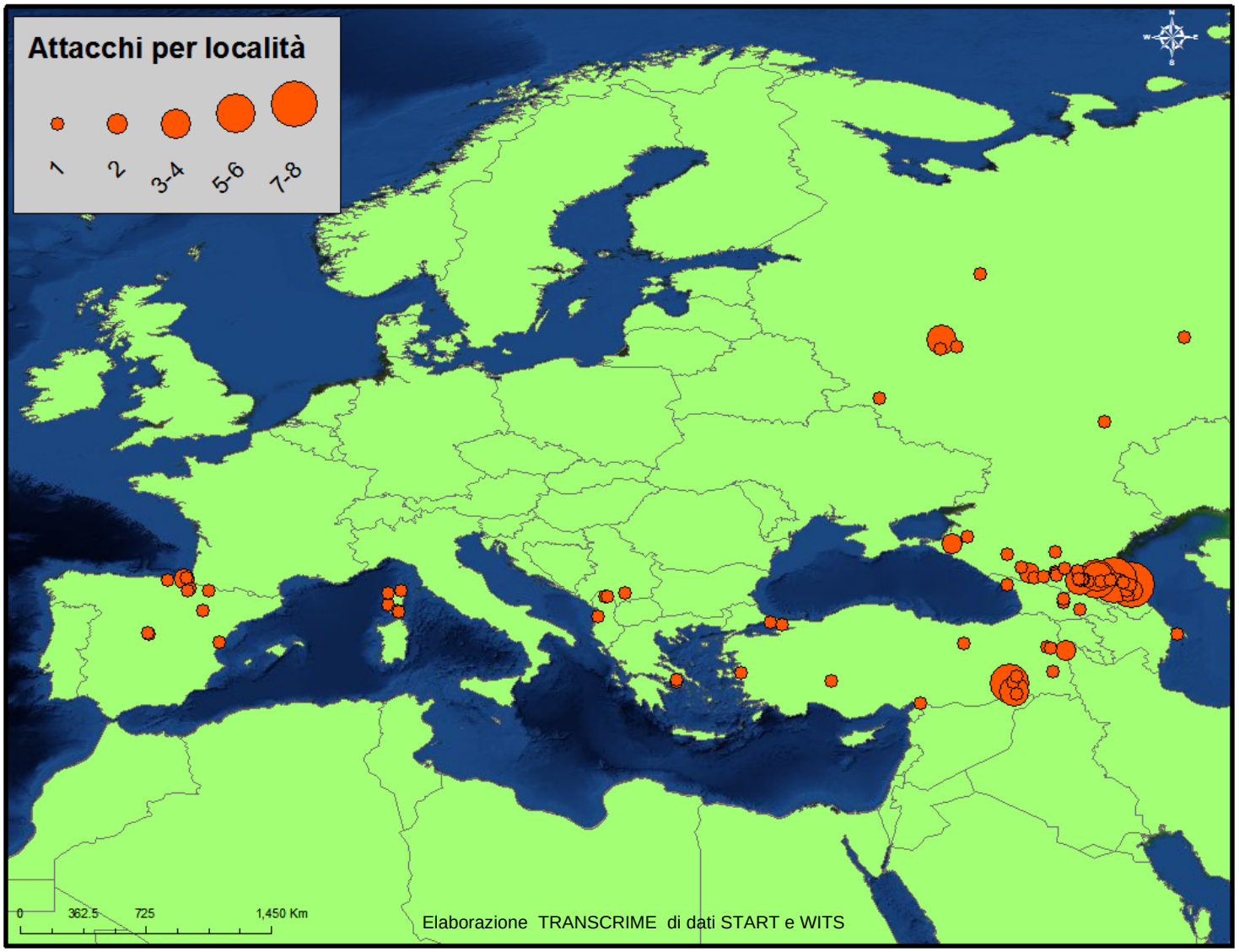

2007
Attacchi per località
1
2
3-4
5-6
7-8
0
365
730
1,460 Km
Elaborazione TRANSCRIME di dati START e WITS

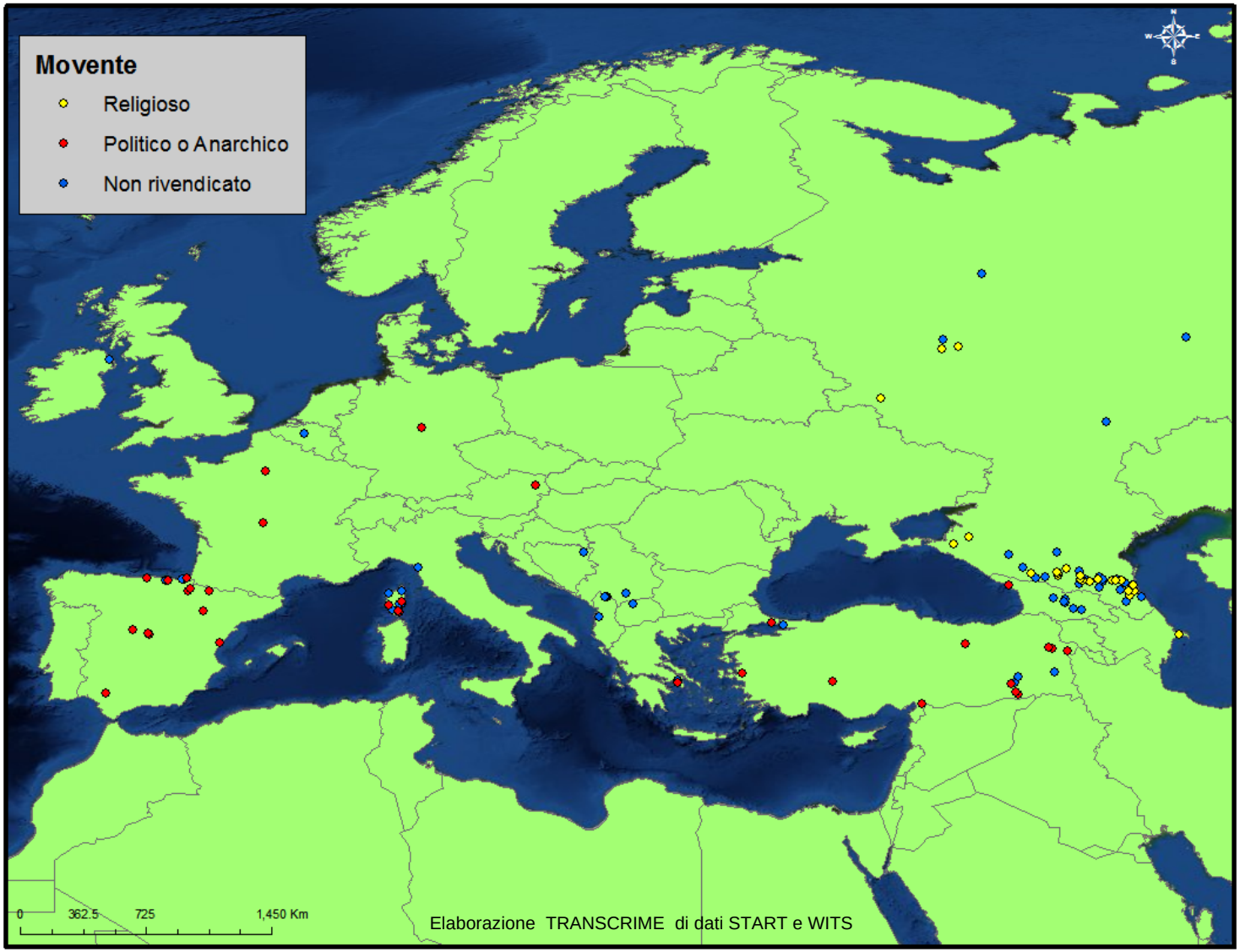

2008
Attacchi per località
1
2
3-4
5-6
7-8
0
365
730
1,460 Km
Elaborazione TRANSCRIME di dati START e WITS


2009
Attacchi per località
1
2
3-4
5-6
7-8
0
365
730
1,460 Km
Elaborazione TRANSCRIME di dati START e WITS

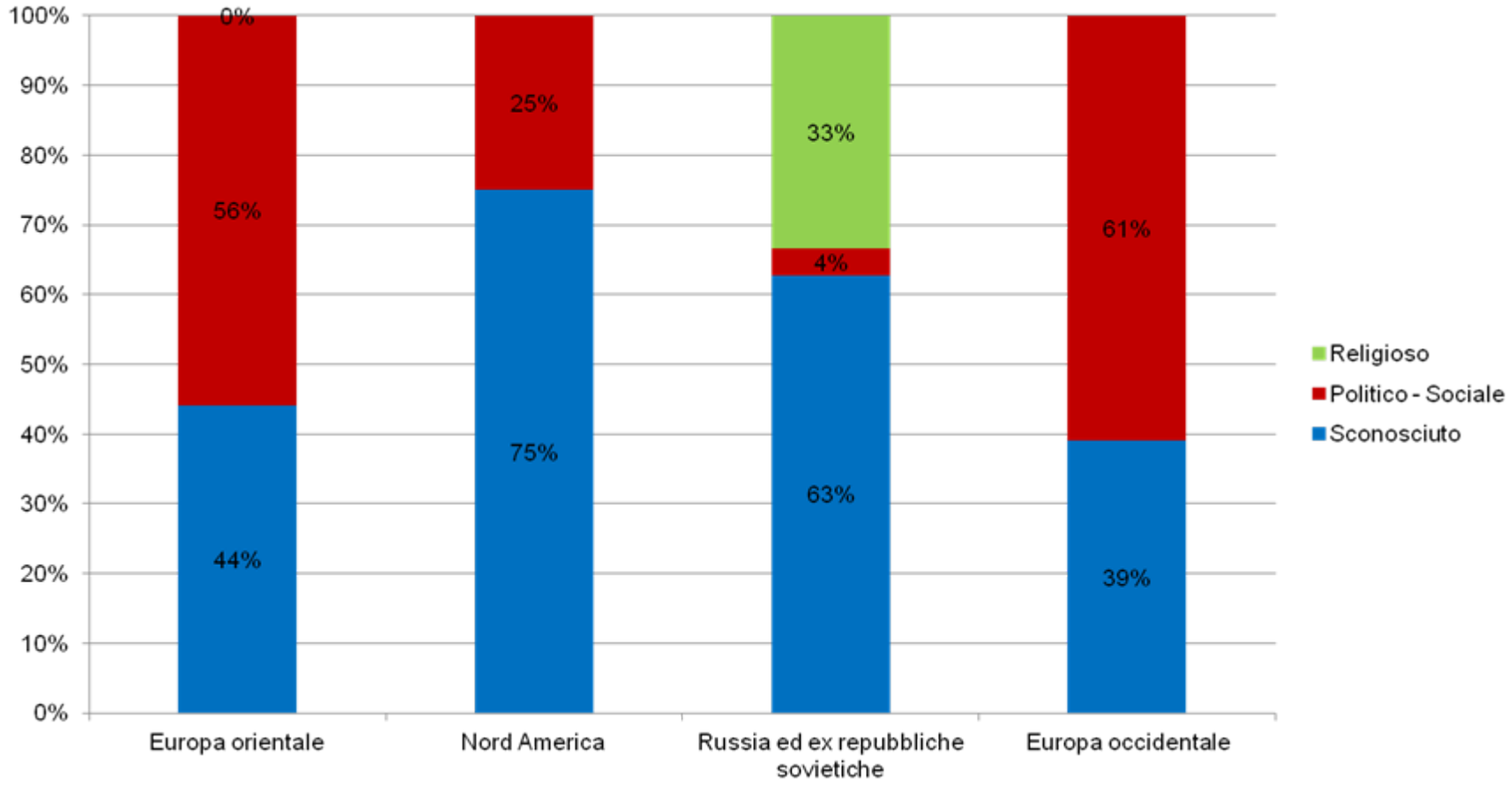

2010
Attacchi per località
1
2
3-4
5-6
7-8
0
365
730
1,460 Km
Elaborazione TRANSCRIME di dati START e WITS


2011
Attacchi per località
1
2
3-4
5-6
7-8
0
365
730
1,460 Km
Elaborazione TRANSCRIME di dati START e WITS


Attacchi per località
1
2
3-4
5-6
7-8
0
362.5
725
1,450 Km
Elaborazione TRANSCRIME di dati START e WITS

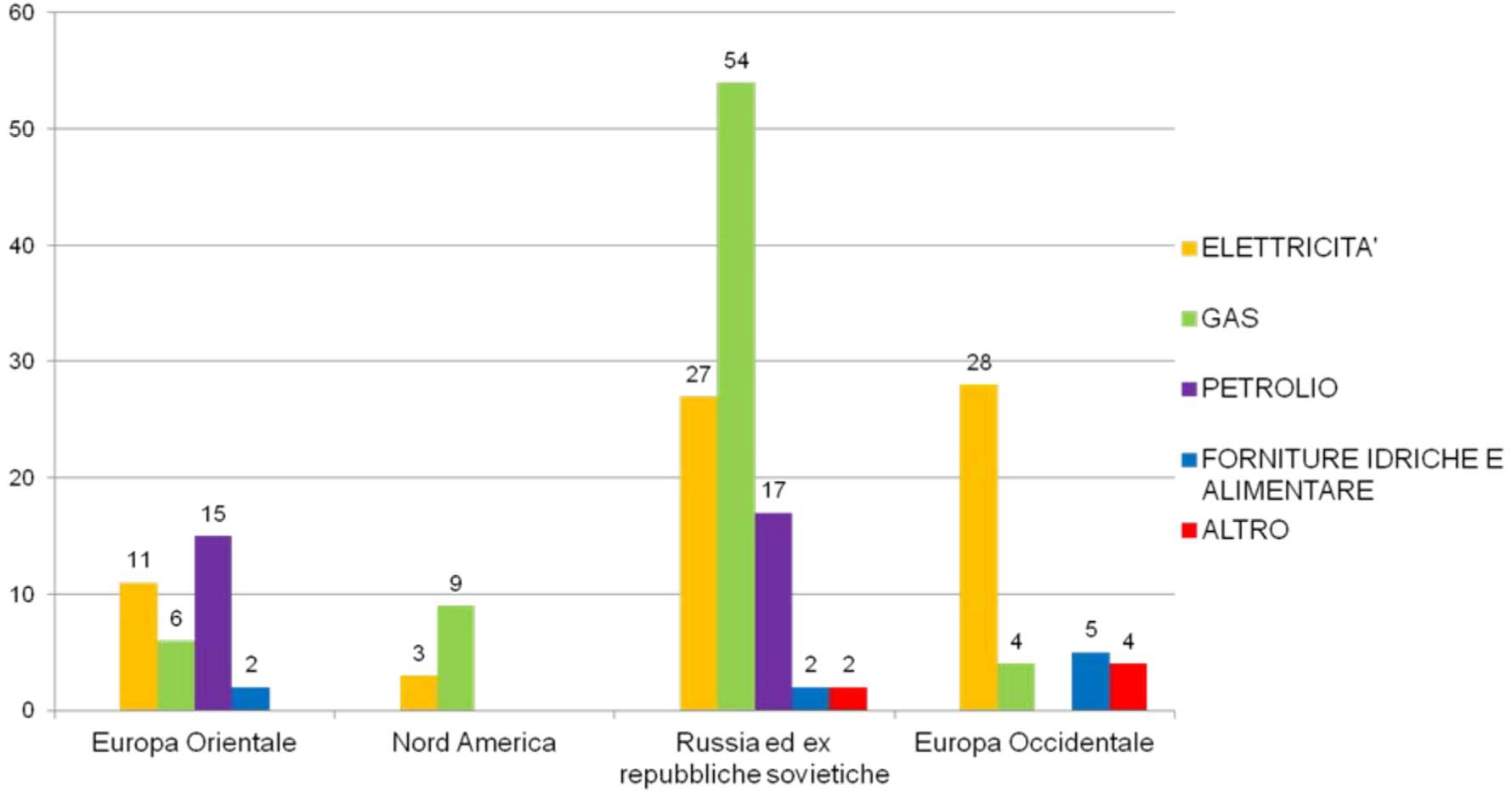

Movente
Religioso
Politico o Anarchico
Non rivendicato
0
362.5
725
1,450 Km
Elaborazione TRANSCRIME di dati START e WITS

Attacchi per tipo di rivendicazione/movente



Elaborazione TRANSCRIME di dati START e WITS

Attacchi a IC per settore specifico



Elaborazione TRANSCRIME di dati START e WITS

2. Le criticità del fenomeno

Cosa rende una IC del settore E&U problematica e vulnerabile?

Cosa rende le IC vulnerabili e appetibili?

Exposed

V

I

L

D

O

N

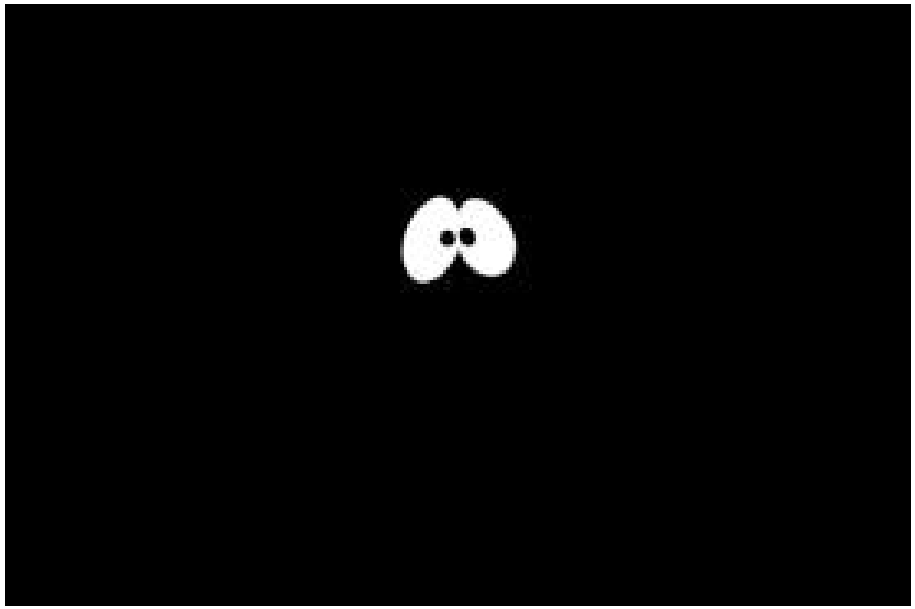
E

(Fonte: Clarke & Newman, 2006)

Cosa rende le IC vulnerabili e appetibili?

Exposed
Vital
I
L

D
O
N
E



(Fonte: Clarke & Newman, 2006)

Cosa rende le IC vulnerabili e appetibili?

Exposed
Vital
Iconic
L

D
O
N
E

(Fonte: Clarke & Newman, 2006)

Cosa rende le IC vulnerabili e appetibili?

Exposed
Vital
Iconic
Legitimate

D
O
N
E

(Fonte: Clarke & Newman, 2006)

Cosa rende le IC vulnerabili e appetibili?

Exposed
Vital
Iconic
Legitimate

Destructible
O
N
E

(Fonte: Clarke & Newman, 2006)

Cosa rende le IC vulnerabili e appetibili?

Exposed
Vital
Iconic
Legitimate

Destructible
Occupied
N
E

(Fonte: Clarke & Newman, 2006)

Cosa rende le IC vulnerabili e appetibili?

Exposed
Vital
Iconic
Legitimate

Destructible
Occupied
Near
E

(Fonte: Clarke & Newman, 2006)

Cosa rende le IC vulnerabili e appetibili?

Exposed
Vital
Iconic
Legitimate

Destructible
Occupied
Near
Easy

(Fonte: Clarke & Newman, 2006)

Analisi Caso 1 – Baksan, Russia, 2010

LOCALITÀ: Baksan, Russia **DATA:** 20/07/2010

TARGET: Centrale Idroelettrica

METODOLOGIA: La centrale è stata attaccata di prima mattina da un nutrito gruppo di fuoco che, dopo aver ucciso le guardie di sicurezza, ha collocato un ordigno esplosivo nei pressi del generatore principale. L'esplosione ha danneggiato il generatore e altre strumentazioni.

RIVENDICAZIONE: Gruppo indipendentista ceceno di ispirazione islamica denominato Caucasus Emirate

EXPOSED:	É una centrale idroelettrica di piccole dimensioni ma centrale e conosciuta nella zona.
VITAL:	Importante per il rifornimento di energia elettrica nelle zone limitrofe.
ICONIC:	Simboleggia la presenza russa in una zona di conflitto.
LEGITIMATE:	Si tratta di un attacco legittimo agli occhi dei terroristi e di chi li sostiene.
DESTRUCTIBLE:	Con l'uso dell'esplosivo è stato molto semplice apportare danni seri alla struttura e ai macchinari. Le piccole dimensioni hanno permesso un risultato maggiore.
OCCUPIED:	L'attacco ha procurato 2 vittime e 2 feriti. L'obiettivo di colpire la gente all'interno è riuscito così come la possibilità di creare disagio agli abitanti della zona.
NEAR:	Estremamente vicina alla zona interessata dal lungo conflitto etnico-religioso in Cecenia. Ciò ha reso facile l'organizzazione dell'attacco e gli spostamenti degli assalitori.
EASY:	L'obiettivo era poco controllato (solo 2 guardie di sicurezza) e quindi facilmente attaccabile.

Analisi Caso 2 - Coaticook, Canada, 2004

LOCALITÀ: Coaticook, Canada **DATA:** 04/12/2004

TARGET: Traliccio alta tensione della linea idroelettrica Quebec – New England

METODOLOGIA: Il traliccio è stato danneggiato con un ordigno esplosivo.

RIVENDICAZIONE: L'attentato è stato compiuto da membri dell' International Resistance Initiative (IRI) gruppo ambientalista, anti-capitalista e anti-americanista.

EXPOSED:	Traliccio facilmente visibile
VITAL:	Fa parte della linea che porta energia all'area di Boston
ICONIC:	Simbolo del trasferimento di risorse da Canada a USA
LEGITIMATE:	L'attacco è connesso alla lotta per contrastare lo sfruttamento delle risorse del Quebec da parte degli Stati Uniti.
DESTRUCTIBLE:	Facile da danneggiare per via delle ridotte dimensioni
OCCUPIED:	Scarsa possibilità di ferire direttamente ma l'obiettivo è creare disagio
NEAR:	Obiettivo facilmente raggiungibile, posto vicino ad una strada
EASY:	Non controllato e facilmente accessibile

Analisi Caso 3 – Bushehr, Iran, 2010

LOCALITÀ: Bushehr, Iran **DATA:** 29/09/2010

TARGET: Centrale nucleare (non ancora operativa)

METODOLOGIA: Attacco informativo tramite il malware Stuxnet.

RIVENDICAZIONE: Non c'è stata alcuna rivendicazione formale anche se la complessità del malware fa ipotizzare che non si tratti dell'azione di un singolo pirata informatico.

EXPOSED:	Obiettivo al centro dell'attenzione perché prossimo all'inaugurazione e a causa del dibattito internazionale sul nucleare in Iran.
VITAL:	Impianto non ancora operativo, ma le potenziali conseguenze sarebbero state molto gravi
ICONIC:	Simbolo dello sviluppo nucleare iraniano
LEGITIMATE:	Il fatto che l'impianto non fosse attivo fa assumere all'attacco una valenza dimostrativa
DESTRUCTIBLE:	Nessun danno fisico all'impianto ma messa a rischio del suo sistema informatico
OCCUPIED:	Centrale non in funzione ma possibili forti rischi in caso di eventi simili in futuro
NEAR:	La distanza è meno importante trattandosi di un attacco informatico
EASY:	Il malware una volta inserito nella rete informatica attraverso una periferica agisce in autonomia

3. Prevenzione e security: spunti di riflessione

Riflessione sui moventi degli attacchi alle IC nel settore E&U e sui nuovi rischi per la security

Alcune considerazioni :

- ✓ **Gli attacchi si concentrano in zone già ad alta tensione sociale/etnica/militare (Caucaso, Corsica, Paesi Baschi, Quebec):** in questo senso l'attacco alle IC ha una funzione strategica all'interno del conflitto
- ✓ La **vicinanza di conflitti militari** influisce sulle **modalità dell'attacco** (a mano armata, esplosione, attentato dinamitardo)
- ✓ Nelle guerre etnico-religiose dell'ex URSS principali target sono IC dell'oil & gas mentre **le Utilities sono prese di mira soprattutto in Europa W&E e America N**
- ✓ Nei paesi occidentali il movente è **principalmente politico/sociale** e legato a **tendenze indipendentiste** (Corsica, Paesi Baschi, Quebec)
- ✓ In pochi casi movente è **'ambientalista':** in questi casi utile riflessione su **percezione pubblica delle IC** e comunicazione utilità/sicurezza IC
- ✓ **Riflessione su recenti attacchi informatici e cyber-security:** possono nascondere moventi/strategie più complesse anche legato a interventi mirati di *security* internazionale