

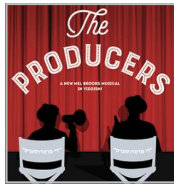


**Israeli Military Razes Family Home of Suspected Palestinian Murderer of a Mother of Six**



**Scandals Loom Over Despite Tel Aviv Attac**

News



**A New Mel Brooks Musical in Yiddish!**  
At the Segal, June 19 to July 10, 2016



BUY TI

Home

# Not Just a Virtual Threat

Aside from the issues of freedom of information, commerce, intellectual property and privacy, the core issue for international lawmakers is the fundamental threat cyberwarfare poses to the present international system, including the law of nations.

Deborah Housen-Couriel

Aug 13, 2010 12:31 PM

 0  Zen

Subscribe

1 Tweet

A recent but minimally reported event may in fact mark a tipping point for a significant global policy initiative.

On July 16, 15 countries, including Israel, with advanced capabilities in the field of cyberattack – that is, the use of computer networks to inflict damage on virtual and real-world targets – presented the UN secretary-general with a report including a framework for cooperative

measures to address digital threats to international security. This initiative, although marked by customary compromise and diplomatic understatement, represents an important step forward in engaging the political will of the global community.

Cyberwarfare and its less sweeping manifestations, such as cybercrime, cyberattack and cyberterror, has in the past decade become less an entertaining quirk of science fiction and much more of a real-world security

issue. It includes a spectrum of activities, some in the virtual realm, some in the physical, and some that overlap: denial-of-service attacks; malware that cripples critical infrastructures; interference with digital networks; and transmission of propaganda or fraudulent military data. No consensual rules of engagement for such activities currently exist.

One example might be an extended shut-down of electrical power in major cities during extreme weather conditions, causing paralysis

of emergency services and water systems. Another might be the electronic scrambling of communications during a humanitarian rescue operation.

Both instances are likely to result in loss of life and physical damage – perhaps even heavier than in a traditional military operation – yet the actions behind them need be no more than keyboard commands.

The international community, led by the United States, China and Russia, began to formally address

the issue in 2005, when UN Secretary-General Kofi Annan appointed the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The group was charged with identifying global cyberthreats and reporting back to the UN, which it did last month. Despite major differences in national approach and political interest, which had stymied earlier efforts, the group's report presents joint recommendations,

including an ongoing effort “to reduce collective risk and protect critical ... infrastructures,” and proposes measures to address cyberattack implications globally.

Aside from the issues of freedom of information, commerce, intellectual property and privacy, the core issue for international lawmakers is the fundamental threat cyberwarfare poses to the present international system, including the law of nations. Article 24)) of

the UN Charter requires states to refrain from the use of force against the territorial integrity and political independence of other states. The Security Council is the arbiter of conflicts that may arise.

Article 51 ensures all countries retain an autonomous right of self-defense “when an armed attack occurs.”

Cyberwarfare, however, can inflict fatal, extensive and irreparable damage upon an enemy without the actual use of physical force or an armed attack. At what point does the state’s



sovereign right  
to self-defense  
from an actual or  
anticipated  
digital attack  
arise? What  
forms may it  
take?

Nations are  
reluctant to  
expose their own  
vulnerability to  
cyberattack,  
although it is  
known that such  
tactics were used  
by NATO in  
Yugoslavia in  
1999, the U.S.  
against Iraq in  
2003, Russia  
against Georgia  
in 2008, and  
Israel in various  
military  
contexts. China's  
2009  
cyberattack on  
Google, although  
commercial in  
nature,  
illustrates its  
potential scale.

Critics treat as alarmist the characterization of cyberattack as an unprecedented security threat. Yet they underestimate the unique and unprecedented qualities of cyberwarfare that are troubling to global lawmakers, including the ubiquitousness of networks accessible to billions; the inherent dual-use nature of targets and weaponry; and, perhaps most ominously, the difficulty of attributing attacks, including proxy attacks, to a particular state

or non-state  
actor.

Several experts  
have advocated  
an approach that  
integrates  
lessons learned  
in the past in  
developing  
international  
regimes that  
govern airborne  
warfare,  
chemical  
weapons and the  
use of space –  
all, in their day,  
innovative  
technologies.

Moreover, in the  
context of  
military doctrine  
and command,  
several countries  
have recently  
established  
cyberwarfare  
capabilities,  
notably the U.S.,  
Britain and  
South Korea.

The protection of  
Israel's national

security interest in cyberspace is not currently a matter of public record, although media reports indicate the Israel Defense Forces' active engagement with this issue. In particular, a public address by Military Intelligence chief Amos Yadlin in February emphasized awareness of the destabilizing potential of cyberattack both globally and regionally. It is likely that here, as elsewhere, protecting critical infrastructures, increasing network redundancy and ensuring deterrence are

major concerns.

In this author's view, Israel's participation in the UN group is an encouraging indication of a proactive outlook on the part of Israeli policy-makers. Additional important steps to be taken include the forging of a cyberwarfare terminology and legal framework that dovetail with emerging international initiatives; and, eventually, the preparation of a national policy document, similar to the recent document on space policy.

The UN report is a positive sign that the

international  
community  
recognizes the  
need for a  
coherent global  
cyberspace  
policy, despite  
conflicting  
national  
interests. This  
initiative should  
aspire to an  
internationally  
recognized  
agreement that  
is focused on  
constraining  
abuse of  
computer  
networks. A  
sense of the new  
vulnerabilities to  
international  
security,  
balanced by the  
tremendous  
potential for  
human  
knowledge and  
interconnection,  
should drive the  
work toward  
both substantive  
legal constraints

and tactical rules  
of engagement.

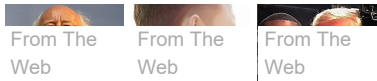
In the words of  
law expert  
Duncan Hollis of  
Temple  
University: New  
tools demand  
new rules.

Deborah  
Housen-Couriel  
is an attorney  
specializing in  
international  
telecommunications  
law, currently  
researching legal  
aspects of  
cyberspace. She  
can be reached at  
housencouriel@gmail.com.

## You Might also Like



Haaretz | Haaretz | Haaretz |  
Jewish Jewish Opinion  
World World Who  
Steven Spielberg Jewish That  
Tells Wedding



**VIEW** Engadget theoryofpost.com

**NIGERIA** Smart 10  
 Top 10 earphone Reasons  
 Richest put AI Why  
 Politicians

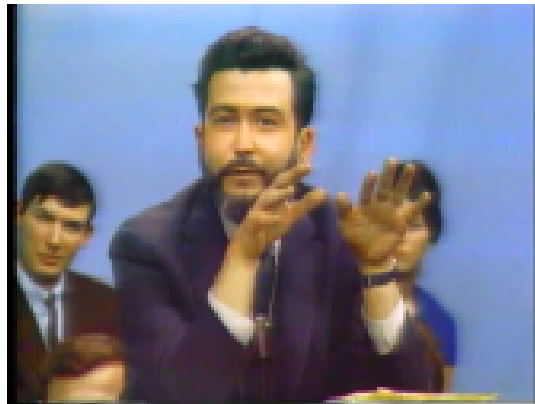
Recommended by

## Comments

**Sign in** to join the conversation.



Nearly 70 Years Later, Disappearance of 1,000 Kids in Israel Remains a Mystery



**This Day in Jewish History // 1925:** A Journalist Who Would Write For, and Be Fired By, the Best Is Born

mp: If Muslims Aren't  
ristians Aren't Either

3

Muhammad Ali's Complicated Relationship With the Jews

an Terrorism Is the End

6

Jenin, Once the Most Militant of Palestinian Refugee Camps, Waves a White Flag



# 9

anti-Semitism in the

## France: Israel's Suspension of Palestinians' Entry Permits Could Escalate Violence



### Swiss Neurobiologist Seeks Thrills as Israeli Answer to Burning Man

By [Liat Elkayam](#) | 10 Hours Ago 🔑



### Two Fallen IDF Soldiers Recognized as 'Missing in Action or Captive'

By Gili Cohen | 19 Hours Ago 🔑

**SPECIAL OFFER**



**Act Now**

... | HAARETZ

An advertisement with a dark blue background. At the top, it says 'E MORE' and 'ARSHIP' in large white letters. Below that, the word 'ONLINE' is visible. A white megaphone graphic is positioned in the center, with the word 'PERSONALIZED.' written inside it in red. At the bottom, there is a white button that says 'EARN YOUR FREE COURSE' with a red play button icon to its right.



[FAQ](#) | [Contact us](#) | [Newsletters](#) | [Terms and conditions](#) | [Privacy policy](#) | [Management](#) | [Editorial](#) | [Accessibility](#) | [Advertise on Haaretz.com](#)

### Israel News

Middle East  
Jewish World  
U.S./World  
Business

### Partnerships

Israel Real Estate  
Dan Hotels in Tel Aviv  
Zalando Rabatkode

### Life

Archaeology  
Science  
Sports

### Culture

Purim  
Books  
Travel  
Theater  
Movies and TV  
Food  
Poem of the Week

### Columnists

Bradley Burston  
Chemi Shalev  
Allison Kaplan  
Sommer  
Anshel Pfeffer  
Sayed Kashua  
Ilene Prusher  
David Rosenberg  
Carlo Strenger  
Vered Guttman  
Mira Sucharov

### Opinion

Daily Cartoon  
Letters to the Editor

### הארץ

חדשות  
גלריה  
ספורט  
ספרים  
מתכונים לשבועות  
סרטים מומלצים  
קפטן אינטרנט

### TheMarker

Finance  
חדשות  
שוק ההון  
צרכנות  
נדל"ן

Haaretz.com, the online edition of Haaretz Newspaper in Israel, and analysis from Israel and the Middle East. Haaretz.com provides extensive and in-depth coverage of Israel, the Jewish World and the Middle East, including defense, diplomacy, the Arab-Israeli conflict, the peace process, Israeli politics, Jerusalem affairs, international relations, Iran, Iraq, Syria, Lebanon, the Palestinian Authority, the West Bank and the Gaza Strip, the Israeli business world and Jewish life in Israel and the Diaspora.

© Haaretz Daily Newspaper Ltd. All Rights Reserved