



Cyber War Crimes

Gresham College
March 30, 2021

Tarah Wheeler

University of Oxford
Harvard University
New America

\$whoami



Search jobs Sign in Search **The Guardian** US edition ▾

News Opinion Sport Culture Lifestyle More ▾

Cyberwar

UK unveils National Cyber Force of hackers to target foes digitally

New unit aims to disrupt online activities of hostile states, terror groups and paedophiles

Dan Sabbagh Defence and security editor

Thu 19 Nov 2020 13:48 EST

f t e



ForeignAffairs.com

Member Login

Trending Transition 2021 Iran Climate Change Coronavirus Afghanistan

from Digital and Cyberspace Policy Program and Net Politics

Indicting Russia's Most Destructive Cyberwar Unit: The Implications of Public Attribution



ZDNet VIDEOS WINDOWS 10 5G CLOUD BEST VPNs GIFT GUIDE SECURITY MORE

On the three-year anniversary of WannaCry, US exposes new North Korean malware

US cyber-security officials expose today three new North Korean malware strains named COPPERHEDGE, TAINTEDSCRIBE, and PEBBLEDASH.

By Catalin Cimpanu for Zero Day | May 12, 2020 -- 16:36 GMT (09:36 PDT) | Topic: Security



Search jobs Sign in Search **The Guardian** US edition ▾

News Opinion Sport Culture Lifestyle More ▾

Cyberwar

Britain has offensive cyberwar capability, top general admits

Gen Sir Patrick Sanders says Boris Johnson has told him to ensure UK is major cyber power

Dan Sabbagh Defence and security editor

Fri 25 Sep 2020 13:00 EDT

f t e



Defense One

THREATS POLICY BUSINESS SCIENCE & TECH IDEAS PODCAST EVENTS INS

About | Newsletter



SCIENCE & TECH

EU's First Cyber Sanctions Target Russian, North Koreans, Chinese Attackers

The EU singled out perpetrators that attacked British hospitals, Ukrainian infrastructure, and the Pyeongchang Olympics.

Search jobs Sign in Search The Guardian US edition

News Opinion Sport Culture Lifestyle More

Cybercrime

Prosecutors open homicide case after cyber-attack on German hospital

Incident in Düsseldorf could be first death caused by a cyber-attack, says UK's former head of cybersecurity



Reuters in Düsseldorf

Fri 18 Sep 2020 12:28 EDT

f t e

Search jobs Sign in Search The Guardian US edition

News Opinion Sport Culture Lifestyle More

Cyberwar

Russian cyber-attack spree shows what unrestrained internet warfare looks like

US indictment of operatives, accused of launching several attacks, gives a detailed account of how they went about their business



Julian Borger in Washington

Mon 19 Oct 2020 19:24 EDT

f t e

FORTUNE RANKINGS MAGAZINE NEWSLETTERS VIDEO PODCASTS CONFERENCES COVID-19 SEARCH SIGN IN Subscribe Now

Most Popular

AstraZeneca COVID-19 vaccine comes under scrutiny again, this time in India

FREE CONTENT

Blockchain opens new business opportunities in travel


Now that Pfizer is the vaccine frontrunner, should you buy the stock?

NEWSLETTERS • DATA SHEET

Is the Düsseldorf cyberattack really the first to result in death?

By ROBERT HACKETT

September 23, 2020 9:25 AM PDT



Emergency Medical Technicians move a gurney out of the emergency entrance into an ambulance at Mt. Sinai Beth Israel Hospital and coronavirus clinic.

JOHN CAMPBELL—GPH (IMAGE)/GETTY IMAGES

German authorities are investigating what may be, as no shortage of media coverage has posited, the world's first death linked to a cyberattack.



“Cybersecurity is one of the only IT roles
where there are people actively trying
to ruin your day, 24/7.”

~ Chris Schueler





“Are cyber war crimes real?”

The domains of war



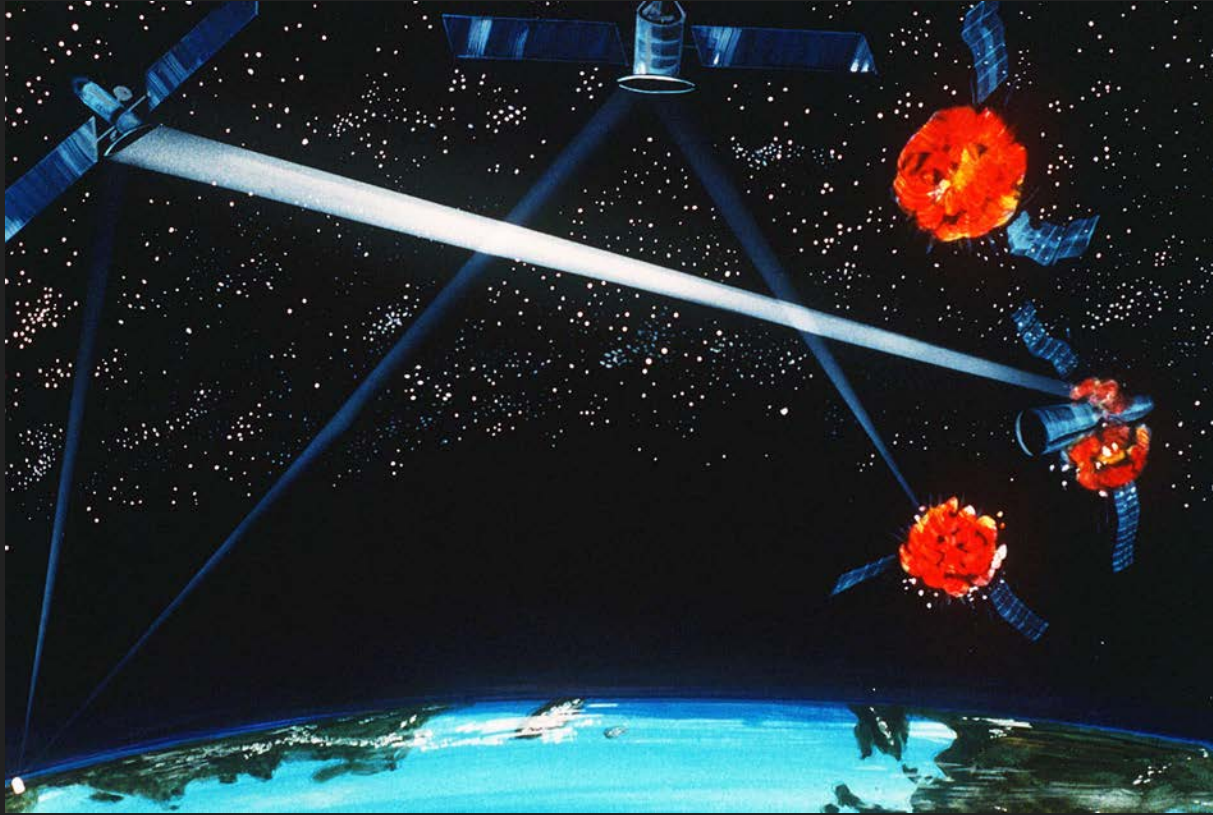
The domains of war



The domains of war



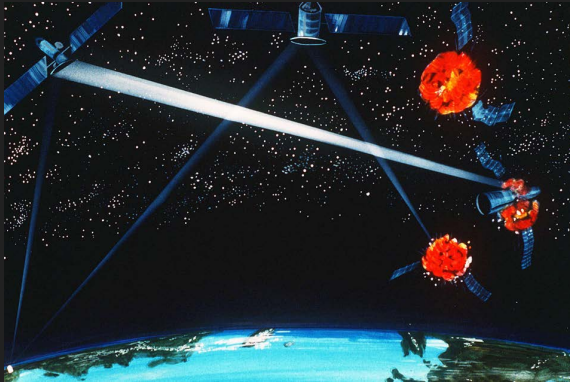
The domains of war



The domains of war



The domains of war



What's (legally) cyberwar?



Cyberwar may be hard to define...

But cyber war crimes are not.

But cyber war crimes are not.

Rome Statute of the International Criminal Court



**Cour
Pénale
Internationale**

**International
Criminal
Court**

Crimes against Humanity

Article 7

Crimes against humanity

1. For the purpose of this Statute, "crime against humanity" means any of the following acts when committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack:
 - (k) Other inhumane acts of a similar character intentionally causing great suffering, or serious injury to body or to mental or physical health.

War Crimes

Article 8²

War crimes

1. The Court shall have jurisdiction in respect of war crimes in particular when committed as part of a plan or policy or as part of a large-scale commission of such crimes.
2. For the purpose of this Statute, "war crimes" means:
 - (a) Grave breaches of the Geneva Conventions of 12 August 1949, namely, any of the following acts against persons or property protected under the provisions of the relevant Geneva Convention:
 - (b) Other serious violations of the laws and customs applicable in international armed conflict, within the established framework of international law, namely, any of the following acts:
 - (i) Intentionally directing attacks against the civilian population as such or against individual civilians not taking direct part in hostilities;
 - (ii) Intentionally directing attacks against civilian objects, that is, objects which are not military objectives;
 - (iv) Intentionally directing attacks against buildings dedicated to religion, education, art, science or charitable purposes, historic monuments, hospitals and places where the sick and wounded are collected, provided they are not military objectives;



Article 5

The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security .

Why don't we just take all this stuff offline



“How is this affecting me?”

What these weapons do

Cyberweapons



```
pe.dwSize = 556;
if ( Process32FirstW(hSnapshot, &pe) )
{
    do
    {
        proc_val = 0x12345678;
        word_count = 0;
        name_len = wcslen(pe.szExeFile);
        do
        {
            cur_pos = 0;
            if ( name_len )
            {
                frame_pos = word_count;
                do
                {
                    enc_byte = &proc_val + (frame_pos & 3);
                    tmp_val = (*enc_byte ^ LOBYTE(pe.szExeFile[cur_pos++])) - 1;
                    ++frame_pos;
                    *enc_byte = tmp_val;
                }
                while ( cur_pos < name_len );
            }
            ++word_count;
        }
        while ( word_count < 3 );
        if ( proc_val == 0x2E214B44 )
        {
            retval &= 0xFFFFFFFF7;
        }
        else if ( proc_val == 0x6403527E || proc_val == 0x651B3005 )
        {
            retval &= 0xFFFFFFFFB;
        }
    }
    while ( Process32NextW(hSnapshot, &pe) );
}
```

Cyberweapons

```
; __int64 __fastcall CreateMSSECSUCProcess()
CreateMSSECSUCProcess proc near

binheritHandles= dword ptr -0C8h
dwCreationFlags= dword ptr -0C0h
lpEnvironment= qword ptr -008h
lpCurrentDirectory= qword ptr -000h
lpStartupInfo= qword ptr -0A8h
lpProcessInformation= qword ptr -0A0h
ProcessInformation= _PROCESS_INFORMATION ptr -98h
StartupInfo= _STARTUPINFOA ptr -78h

push    rbx
sub     rsp, 0E8h
xor     eax, eax
xor     ebx, ebx
lea     rcx, [rsp+0E8h+StartupInfo.lpReserved] ; Dst
lea     r8d, [rbx+60h] ; Size
xor     edx, edx ; Val
mov     [rsp+0E8h+ProcessInformation.hProcess], rbx
mov     [rsp+0E8h+ProcessInformation.hThread], rax
mov     qword ptr [rsp+0E8h+ProcessInformation.dwProcessId], rax
call    memset
lea     rax, [rsp+0E8h+ProcessInformation]
lea     rdx, Dst ; lpCommandLine
xor     r9d, r9d ; lpThreadAttributes
mov     [rsp+0E8h+lpProcessInformation], rax ; lpProcessInformation
lea     rax, [rsp+0E8h+StartupInfo]
xor     r8d, r8d ; lpProcessAttributes
mov     [rsp+0E8h+lpStartupInfo], rax ; lpStartupInfo
mov     [rsp+0E8h+lpCurrentDirectory], rbx ; lpCurrentDirectory
mov     [rsp+0E8h+lpEnvironment], rbx ; lpEnvironment
xor     ecx, ecx ; lpApplicationName
mov     [rsp+0E8h+dwCreationFlags], 8000000h ; dwCreationFlags
mov     [rsp+0E8h+StartupInfo.cb], 68h
mov     [rsp+0E8h+binheritHandles], ebx ; binheritHandles
mov     [rsp+0E8h+StartupInfo.wShowWindow], bx
mov     [rsp+0E8h+StartupInfo.dwFlags], 81h
call    cs:CreateProcessA
test    eax, eax
jz      short loc_180001198
```



Cyberweapons

```
_initterm(&DAT_0040b000,&DAT_0040b008);  
local_78 = *(byte **)_acmdln_exref;  
if (*local_78 != 0x22) {  
    do {  
        if (*local_78 < 0x21) goto LAB_00409b09;  
        local_78 = local_78 + 1;  
    } while( true );  
}  
do {  
    local_78 = local_78 + 1;  
    if (*local_78 == 0) break;  
} while (*local_78 != 0x22);  
if (*local_78 != 0x22) goto LAB_00409b09;  
do {  
    local_78 = local_78 + 1;  
LAB_00409b09:  
} while ((*local_78 != 0) && (*local_78 < 0x21));  
local_60.dwFlags = 0;  
GetStartupInfoA((LPSTARTUPINFOA)&local_60);  
GetModuleHandleA((LPCSTR)0x0);  
local_6c = FUN_00408140();  
/* WARNING: Subroutine does not return */  
exit(local_6c);  
}
```





“What can I do about it?”

0%

Amount of security that is perfect.

Or will ever be perfect.

26%

Companies that were vulnerable to WannaCry in
2017

That still are.

100%

Companies with current vulnerabilities and
ongoing incidents



“What can I do about it?”

“No one really wants backups...
What they want is *restore*.”

~Elizabeth Zwicky

Data Retention

TRAITS

- Never shrinks
- Only grows
- Metadata counts
- Sensible data retention is governed not by technological limits, but by compliance and regulation

IMPLICATIONS

- No option to delete fully
- Metadata can effectively replicate the use of most data in communications even without the data itself

Data Backup

TRAITS

- Offsite
- Not constant and continuous integration with production systems
- Not necessarily production data; can be forensically stored HDDs or other data that must be physically walked

IMPLICATIONS

- Not physically accessible by knowledge workers processing GDPR/Chinese/USG requests for warrants or deletion
- Only available through an interface

Data Restore

TRAITS

- Multiple physical DCs and generally at least one onsite storage replicating to offsite
- constant and continuous integration with production systems
- Often provided by third party software or through API
- Often in a proprietary format (duplicity) or in OSS format but difficult to work with (rsync)

IMPLICATIONS

- Metadata generated and often stored on access to data for China/GDPR/USG requests for info or deletion
- Often available onsite for internal requests
- Often owned by multiple teams and contributed to by multiple teams
- Often owned by IT or office of the CIO, and often not audited by CISO's office



“What can I do about it?”

The multitude of choices in data architecture to provide for security are sometimes in **direct conflict** with privacy.

The overwhelming conflict can cause a **hands-in-the-air approach** to developing data structures with both privacy for regulation and security for ethics.

Are doctors **responsible** for keeping patient data safe? If not doctors, who? If you ask your doctor **what happens to my data**, how would they answer?

All personal data will eventually either be deleted or will be **fully public** and in the hands of a foreign power.



Data, Tomorrow (what
do I not know that I
don't know)

The World's First AI-powered Cyberattack

Era of AI-Powered Cyberattacks Has Started

The growing sophistication of fast-moving cyberattacks is forcing companies to employ similar technologies to defend themselves

the use of AI and machine learning in cyber breaches opens up a range of dangerous scenarios, from the ability of intruders to more easily scan networks for unpatched ports to the automated composition of emails that match the tone and writing style of someone that the intended target knows.

Automated Spearphishing at Scale

Equifax had one job — keep its vast trove of personal financial information on millions of Americans secure. In 2017, the company failed spectacularly at that job when a hack compromised the information of more than [147 million people](#).

SECURITY | LEER EN ESPAÑOL

Massive breach leaks 773 million email addresses, 21 million passwords

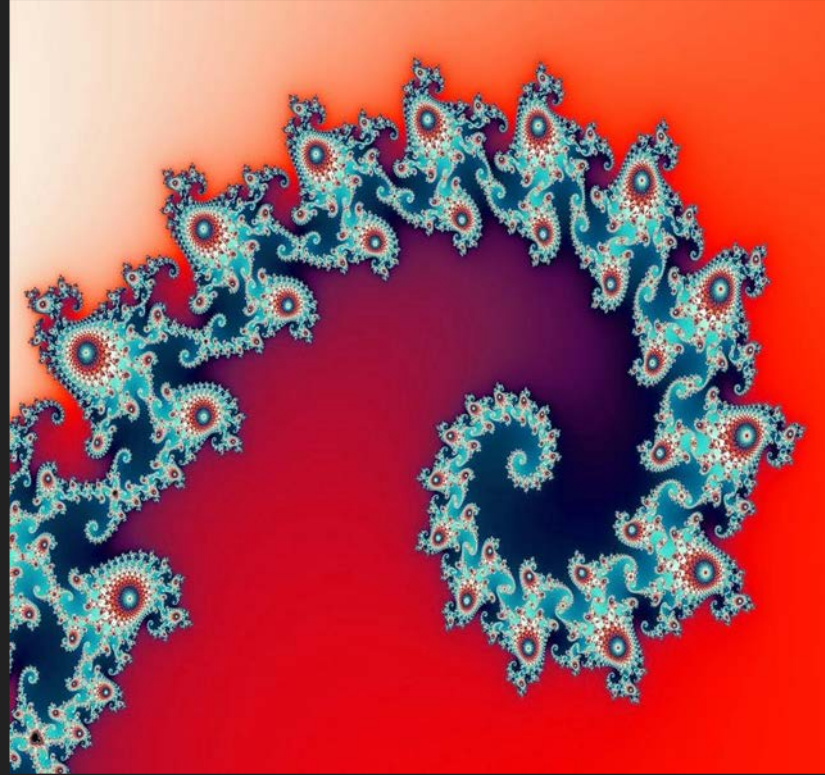
The best time to stop reusing old passwords was 10 years ago. The second best time is now.



Trends in Automated Warfare



This Won't End... Ever.



So make it something that gets better over time.



Thank You



twitter	@tarah
email	t@tarah.org
web	https://tarah.org
instagram	@tarahwheeler
linkedin	/tarah
facebook	/tarahwheeler