NICE Conference and Expo 2022

JUNE 6 - 8, 2022 | WESTIN PEACHTREE PLAZA | ATLANTA, GA

DEMYSTIFYING CYBERSECURITY

Integrated Approaches to Developing Career Pathways







DIAMOND



THANK YOU SPONSORS



MOBILE APP



CYBER



LOCAL HOST PARTNER



CONFERENCE BAG





SANS

REGISTRATION

GIAC





WELCOMING REMARKS

Randy Pestana

Director of Education and Training for Cybersecurity@FIU Florida International University

Conference Emcee







CONFERENCE WELCOME

Brian Fonseca

Executive Director of Cybersecurity@FIU Director of Jack D. Gordon Institute for Public Policy Florida International University

Kenneth A. Jessell

Interim President Florida International University







DIAMOND



THANK YOU SPONSORS



MOBILE APP



CYBER



LOCAL HOST PARTNER



CONFERENCE BAG





SANS

REGISTRATION

GIAC





NICE CONFERENCE WELCOME

Rodney Petersen

Director

National Initiative for Cybersecurity Education, NIST in the U.S. Department of Commerce





Together Again

NICE Mission:

To energize, promote, and coordinate a robust community **working together** to advance an integrated ecosystem of cybersecurity education, training, and workforce development



NICE Values | Working Together

- Foster communication
- Facilitate collaboration
- Share and leverage **resources**
- Act based on evidence
- Evaluate and improve
- Challenge assumptions
- Stimulate innovation
- Model inclusion





National Cybersecurity Education Month

Individuals and organizations are invited to:

- 1. Recognize the role of cybersecurity education
- 2. Support Federal, State, and local efforts

Congress commits to:

- 1. Raising awareness about cybersecurity education
- 2. Taking legislative action in support of cybersecurity education to build and sustain the cybersecurity workforce

117th CONGRESS 2d Session	S. RES.
Designating June 2	2022 as "National Cybersecurity Education Month".
IN THE SE	ENATE OF THE UNITED STATES
	self and Ms. ROSEN) submitted the following resolution red to the Committee on
R	ESOLUTION
	LOOLUTION

- Whereas recent cyberattacks and vulnerabilities present cybersecurity risks to individuals and organizations and increase the urgency to grow and sustain a knowledgeable and skilled cybersecurity workforce in both the public and private sectors;
- Whereas, according to CyberSeek.org, as of 2022, there are 597,767 open jobs in cybersecurity in the United States and 1,053,468 individuals in the cybersecurity workforce;
- Whereas a 2017 report entitled "Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce:
 Building the Foundation for a More Secure American Future", transmitted by the Secretary of Commerce and the Secretary of Homeland Security, proposed a vision to

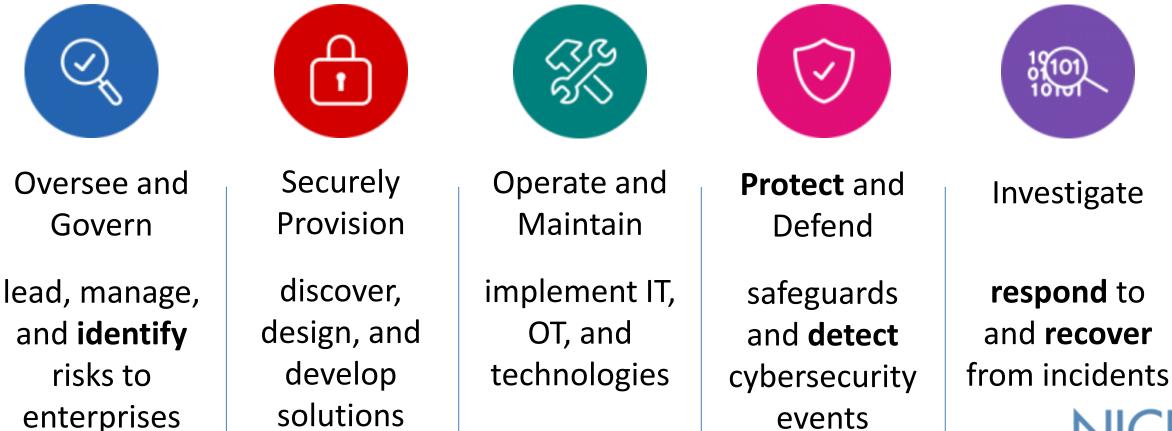


DEMYSTIFYING CYBERSECURITY

Integrated Approaches to Developing Career Pathways

Demystifying Cybersecurity Careers | Setting a Destination

Varieties of Careers Included in NICE Framework:



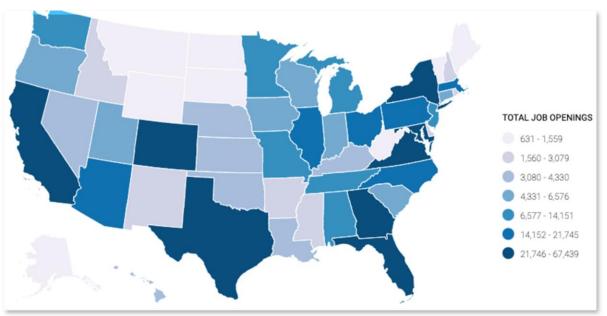
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NEW CyberSeek Data

Total Cybersecurity Job Openings:

714,548

(compared with 597,767)



perate & Maintain Oversee & Govern Protect & Defend 474,768 329,318 279,062 Securely Provision 443,726 Analyze Collect & Operate 194,017 82,103 Investigate 53,210



CyberSeek.org

NEW CyberSeek Data

Total Employed Cybersecurity Workforce:

1,091,576

(compared with 1,053,468)





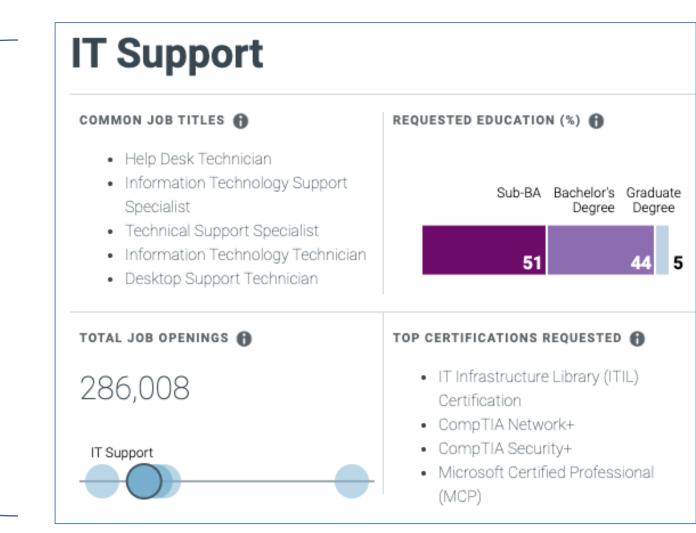


CyberSeek Career Pathway

IT Support

IT Support Job openings 286,008

Click the circle for more info





CyberSeek.org

Learn More

TOMORROW June 8th | 11-11:30 AM

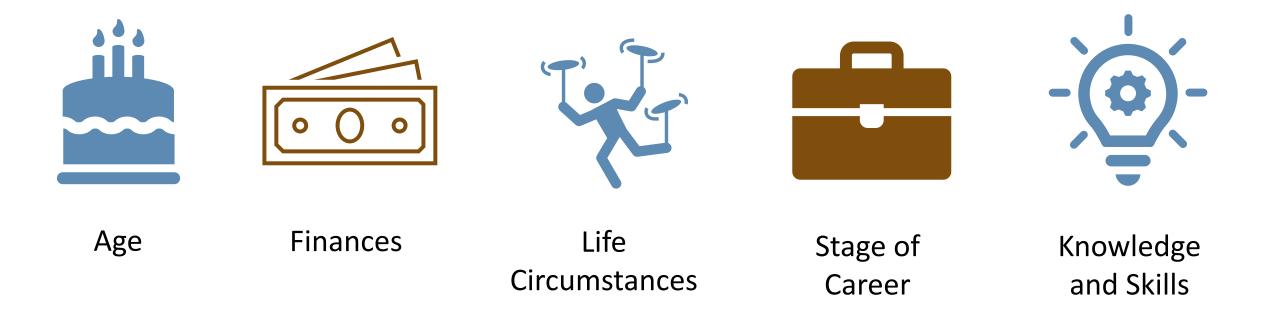
What Does CyberSeek Data Tell Us About the Challenge and Opportunity Ahead?



Exhibit Hall |Seventh Floor - Augusta Ballroom



Demystifying Cybersecurity Careers | Confirming Your **Starting Point**





Demystifying Cybersecurity Careers | Selecting Your Route(s)





Cybersecurity Apprenticeship Awareness and Program Development







Multiple Pathways to Cybersecurity CareersStarting PointsRoutesDestinations

Department of Commerce Secretary Raimondo's Workforce Principles

Highly Effective Workforce Investments:

- Are employer led
- Are guided by multiple community partners
- Include wrap-around services
- Increase diversity, equity, and inclusion
- Prioritize proven earn and learn models
- Lead to stackable, industry-recognized credentials

- Measure and evaluate outcomes
- Build sustainable systems and partnerships
- Connect workforce development to economic development
- Are coordinated
- Encourage the use of other government and private funding



Coming in 2022-23 – RAMPS Communities

RAMPS communities are:

- employer led
- include multiple community partners
- advance DEIA goals
- prioritize apprenticeships
- lead to stackable credentials
- measure outcomes
- build sustainable systems
- leverage multiple funding sources



Vision

Prepare, grow, and sustain a cybersecurity workforce that safeguards and promotes America's national security and economic prosperity.



We are STRONGER TOGETHER





CONFERENCE WELCOME

Jon Brickey Senior Vice President Cybersecurity Evangelist Mastercard

Bridgett Paradise Chief People and Culture Officer Tenable





NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION



NICE Community Coordinating Council

Jon Brickey Mastercard Bridgett Paradise Tenable

Overview of the NICE Community Coordinating Council

The NICE Community Coordinating Council (NICE Community) has been established to provide a mechanism in which *public* and *private* sector participants can develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development.



NICE Strategic Plan and Implementation Plan



NICE Strategic Plan

Email: nice@nist.gov Website: www.nist.gov/nice





Talent Management

NICE

Research

Workforce

Transform Learning to Build and

Sustain a Diverse and Skilled

Promote the Discovery of

Cybersecurity Careers and

Multiple Pathways

Modernize the Talent Management Process to Address Cybersecurity Skills Gaps

Expand Use of the Workforce Framework for Cybersecurity (NICE Framework)

Drive Research on Effective Practices for Cybersecurity Workforce Development



Project Teams

Multiple Career Pathways for Cybersecurity

Improve the Quality and Availability of Credentials

Incorporating Cybersecurity into a Public Service Education Cybersecurity Career-Entry Guidance for Employers and Job-Seekers





Bridgett Paradise

Chief People & Culture Officer, Tenable

Incoming Industry Co-Chair,

NICE Community Coordinating Council



Engage with the NICE Community Coordinating Council *at the NICE Conference & Expo 2022*

TODAY June 7th | 10am **Meet and Greet** Co-Chairs of NICE Community Coordinating Council

NICE Exhibit Booth

TODAY June 7th | 1:30pm

Communities of Interest

- Apprenticeships
- Competitions
- K12
- NICE Framework

Birds of a Feather

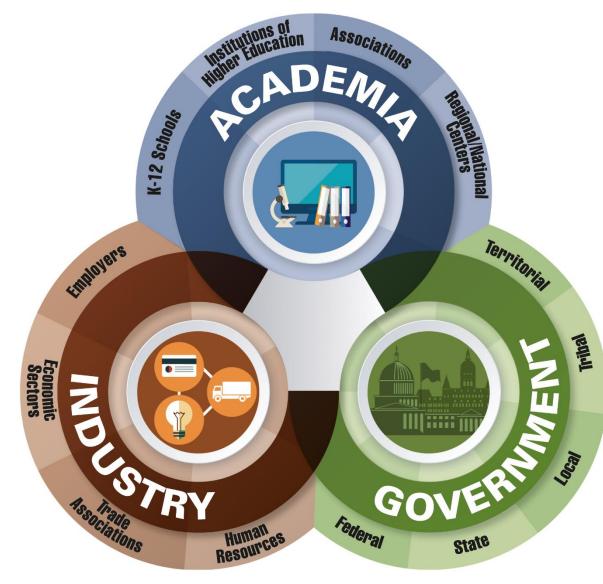
TOMORROW June 8th | 1:30pm

Working Groups

- Career Discovery
- Transform Learning
- Modernize Talent Management



Networking Breakouts



nist.gov/nice/community



SECTOR BASED APPROACHES TO CYBERSECURITY EDUCATION, TRAINING AND WORKFORCE DEVELOPMENT Jennifer Kutz Cybersecurity Portfolio/Program Manager Victoria's Secret & Co.

Robert Grillo Vice President & CIO Florida International University

Lonnie Harris Vice President of Privacy Engineering Equifax

Moderator: Marian Merritt

Deputy Director National Initiative for Cybersecurity Education, NIST in the U.S. Department of Commerce

FICTIONAL INTERNATIONAL UNIVERSITY





CONFERENCE OVERVIEW

Raquel Hill

Chair of the Computer and Information Science Dept. Spelman College

Austin Cusak

Cyber Defense Education and Training Cybersecurity and Infrastructure Security Agency

Brian Correia Director of Business Development SANS







EXHIBIT HALL BREAK

Augusta Ballroom, 7th Floor 10:00 a.m. – 10:30 a.m.







BREAKOUT SESSIONS

10:30 a.m. - 11:15 a.m.

Building and Sustaining a Statewide Cybersecurity Education and Workforce Development Ecosystem 6th floor, Chastain 1 & 2

The Cybersecurity Education Initiative 6th floor, Chastain D & E

Innovation Pilot of HBCU Apprenticeship Cohorts 6th floor, Chastain F & G

Talent Mobility: An Essential Defense Against the Great Reshuffling 6th floor, Chastain H,I,&J







BREAK

11:15 a.m. – 11:30 a.m.







BREAKOUT SESSIONS 11:30 a.m. - 12:15 p.m.

Breaking Bread: A Recipe for Standing Up an Entry-Level Cyber Talent Program 6th floor, Chastain 1 & 2

A Holistic Approach to Developing the Next Generation of Diverse Cybersecurity Professionals with Multi-Organizational Partnerships 6th floor, Chastain D & E

IT and Cybersecurity Degree Apprenticeship Cohorts at HBCUs 6th floor, Chastain F & G

Going for the Gold! Insights and Lessons Learned from Coaching the First Ever US Cyber Games Team 6th floor, Chastain H,I,&J







LUNCH

Peachtree Ballroom 12:15 p.m. – 12:45 p.m.







LUNCHEON KEYNOTE

Roy Zur CEO, Founder of Cybint Solutions ThriveDX SaaS





hrivedx

Solving The Cyber Talent Shortage And Skills Gap In Cybersecurity

NICE Conference and Expo

A Leak in the Dike

BY PHOEBE CARY

And the boy! He has seen the danger, And, shouting a wild alarm, He forces back the weight of the sea With the strength of his single arm! He listens for the joyful sound Of a footstep passing nigh; And lays his ear to the ground, to catch The answer to his cry. And he hears the rough winds blowing, And the waters rise and fall, But never an answer comes to him, Save the echo of his call. He sees no hope, no succor, His feeble voice is lost; Yet what shall he do but watch and wait, Though he perish at his post!

Hans Brinker A classic Dutch adventure

Text Martijn de Rooi Illustrations Nicolas Trottier

The Cyber Talent Shortage & Skills Gap

The World is facing a massive deficit of qualified cyber talent affecting national security and economic stability. Traditional approaches to education are not solving the problem



Unfilled jobs globally in cybersecurity as of 2022 (Cybersecurity Ventures)



The estimated costs of cyber crimes to the world by 2025 (Cybersecurity Ventures) 435%

Increase in ransomware since 2020 (ESI-THOUGHTLAB Research) **95**%

Of all cybersecurity incidents involve the human-factor (IBM Cybersecurity Report)



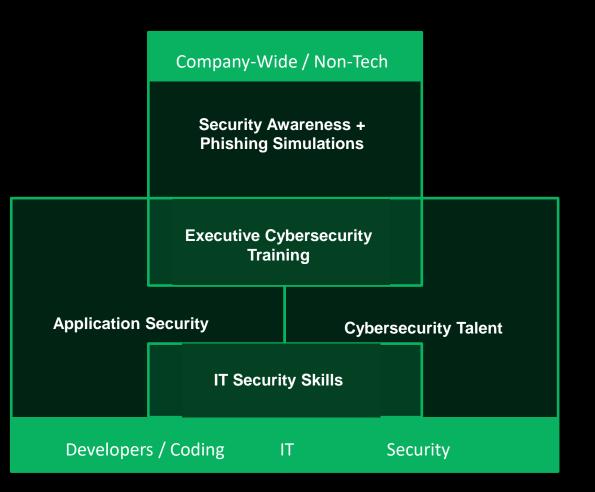
Beyond Awareness

Addressing the cybersecurity talent shortage and skills gap in every level of the organization:

Company-Wide Engineers & Developers IT & Security

Executives

360' View - Human Factor





A New Approach - A New Category

Real World End-to-End Cyber Security Training & Education

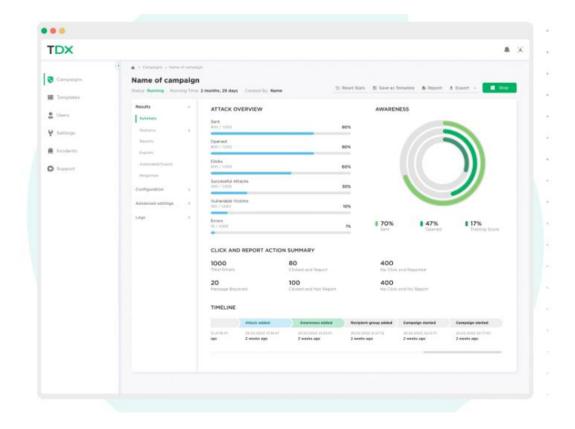
From Classroom to Boardroom



Security Awareness & Phishing

95% of cyber attacks involve human error IBM Cyber Security Report

Advanced Real-World Attack Simulations Based On Multiple Attack Vectors. From Phishing To Spear-Phishing





Application Security Training

84% of attacks are carried out in the application layer

Only 15% of dev teams participate in formal security training - ESG

Real-World AppSec & Secure-Code Training In Real-Time On Emerging Threats. Created By Developer For Developers

← Misconfigured AWS ← Cognito Attributes	HTTP REQUEST	
6. Intercept Request		
To reverse-engineer the authentication logic, Bob		
browser using an application web proxy.		
Note		
What is a web proxy?		
A web proxy, also known as an HTTP proxy is a		
HTTPS traffic between their machine and a remote web application. This may include HTTP/HTTPS		
request and response data, request parameters,		
Instructions		
the second se		



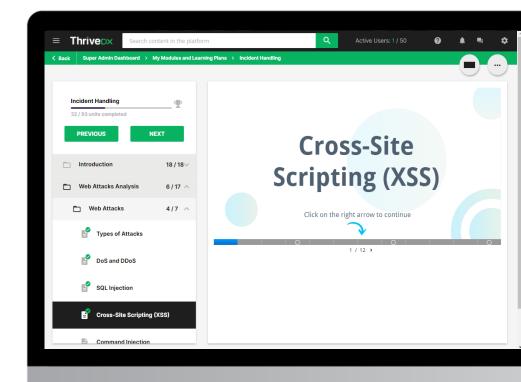


Cybersecurity Bootcamps

3.5M unfilled jobs in cybersecurity as of 2022 - Cybersecurity Ventures

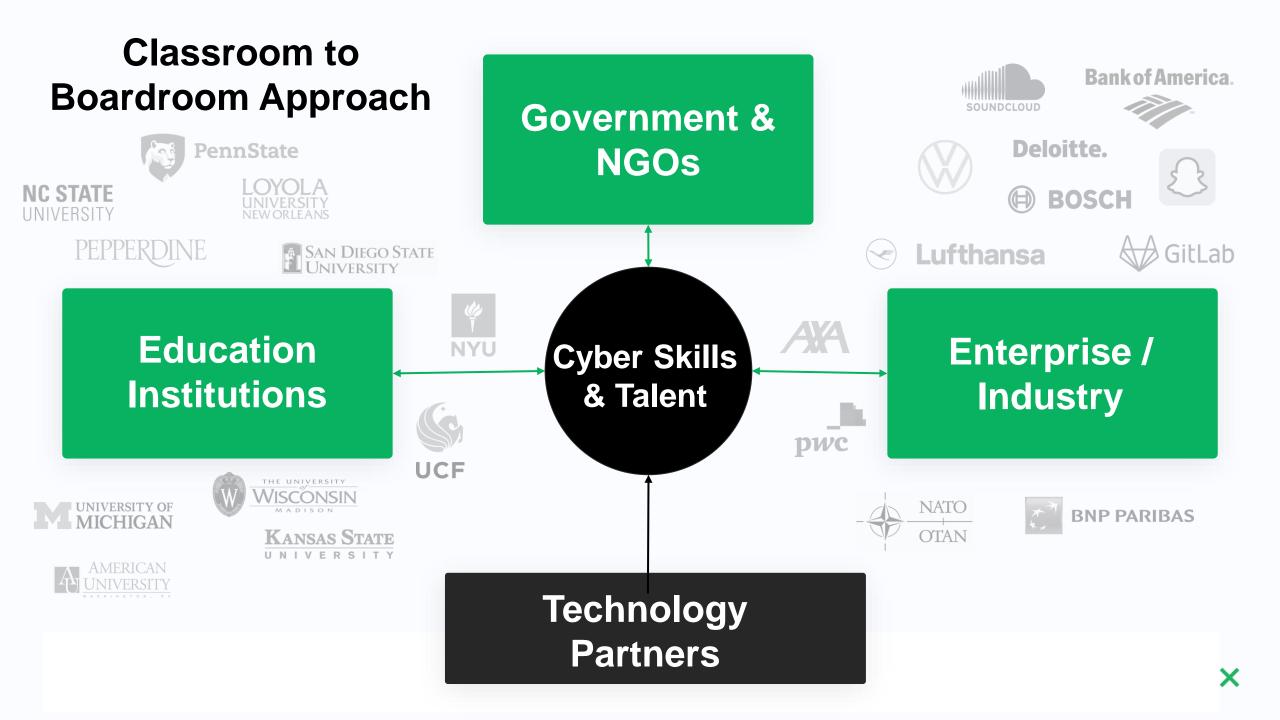
69% of leaders struggle with cyber hiring and see diversity as a main Challenge - Fortinet Cyber Skills 22

Hands-On Cybersecurity Bootcamps. Training, Assessing & Matching Diverse Talent With Enterprise And Government Needs









ThriveDX by the Numbers

Enterprise Users

+10M

+50k Bootcamp Graduates

+500

Enterprise Customers



Education Institutions

+50%

Learners from Diverse Communities



Hiring Partners



Let's Join Forces -Reskilling the Workforce & Upskilling the Industry





LUNCHEON KEYNOTE

Paul Bingham

Vice President & Dean of College Information Technology Western Governors University



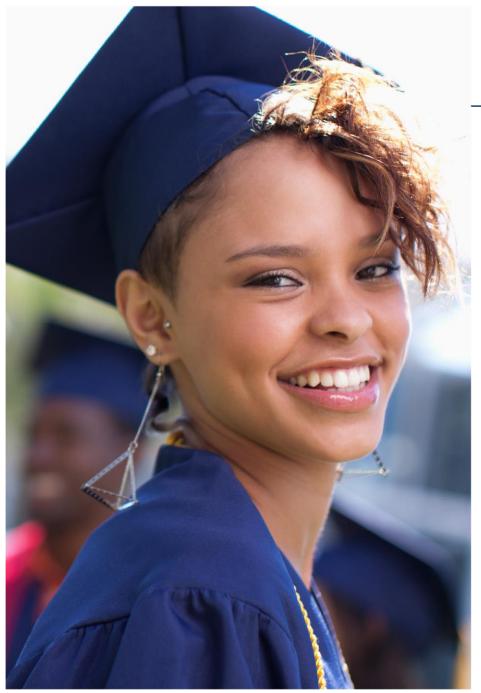


THE FUTURE CYBERSECURITY WORKFORCE

NICE Conference Atlanta, GA June 7, 2022







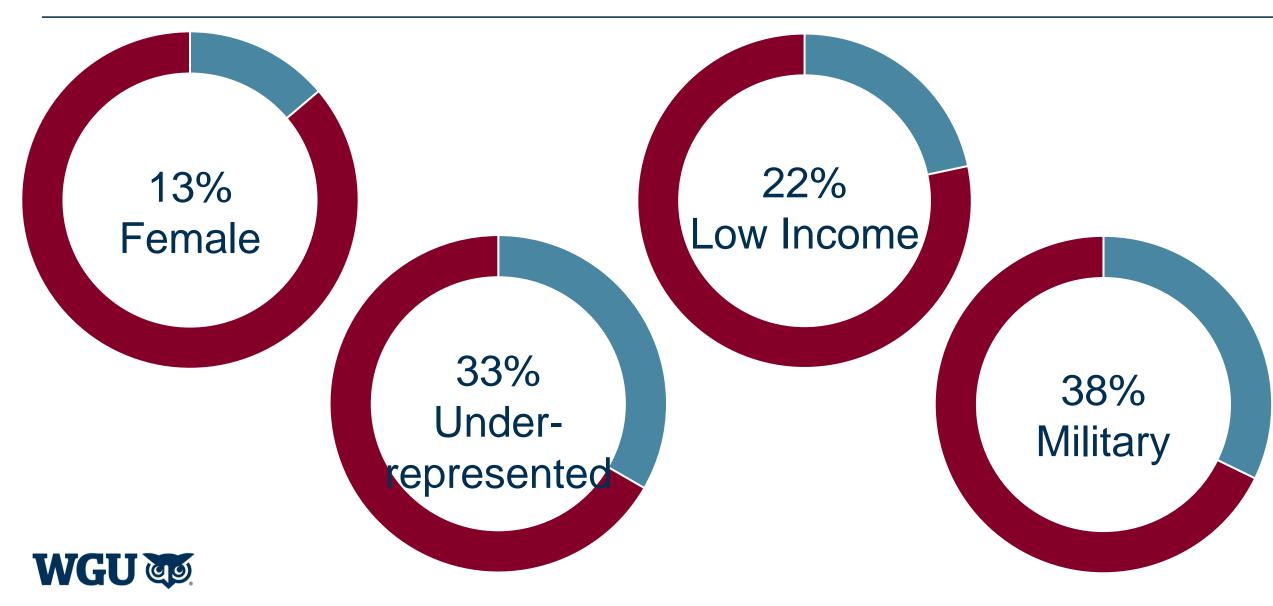








OUR STUDENT POPULATION...

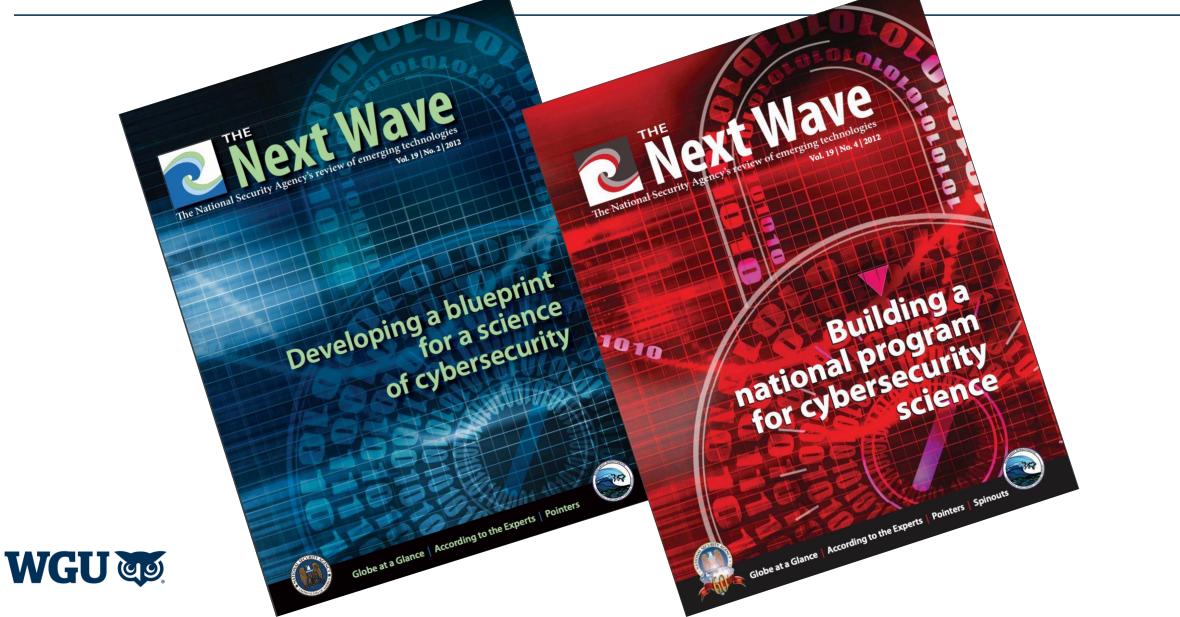


FUTURE CYBERSECURITY PROFESSIONALS...





BACK TO THE FUTURE...



BACK TO THE FUTURE...

Developii

01

Globe at a Glance | Accord

The National Security Agence

THE

The National Security A

ovt Wave

Femerging techni

Building a science

Globe at a Glance | Pointers | From Lab to Market

of cybersecurity.

The next move

[a] 19 No

uilding a program rsecurity

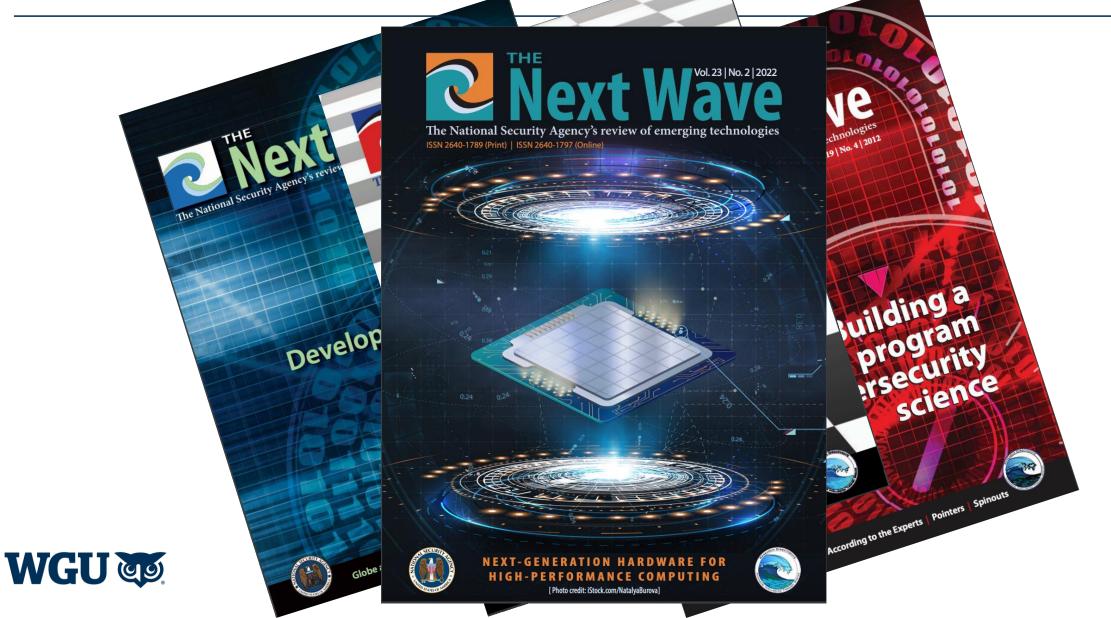
Globe at a Glance | According to the Experts | Pointers | Spinouts

science

ान



BACK TO THE FUTURE...



FUTURE CYBERSECURITY PROFESSIONALS...

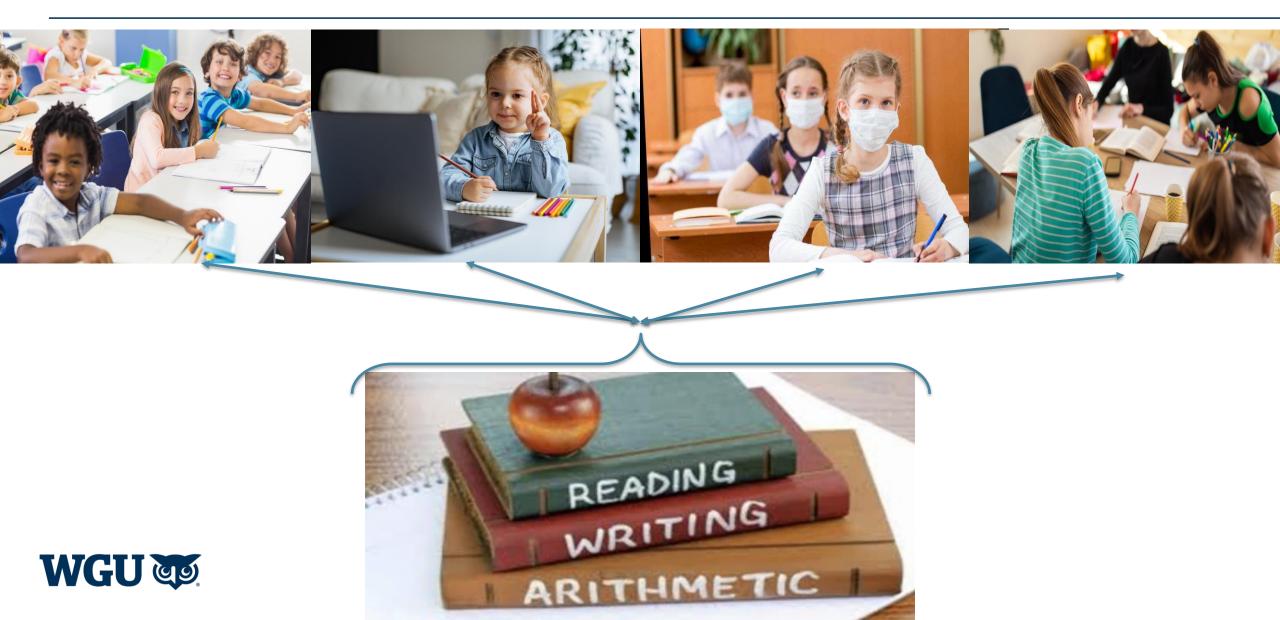




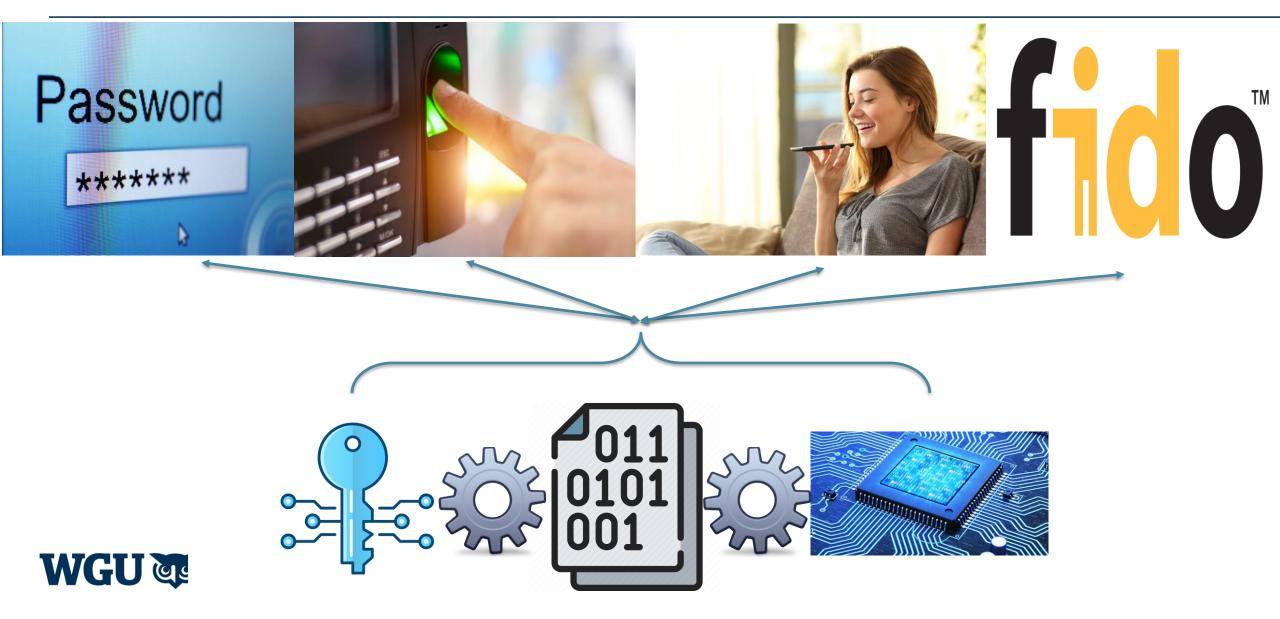
AUTOMATION



ADAPT TO CHANGE



ADAPT TO CHANGE



COLLABORATION





Thank you, NICE Conference attendees!

Stop by Booth #1 to learn more about WGU's Cybersecurity programs



WESTERN GOVERNORS UNIVERSITY_®



BREAK

1:15 p.m. – 1:30 p.m.







BIRDS OF A FEATHER 1:30 p.m. - 2:15 p.m.

K12 Cybersecurity Education 6th floor, Chastain 1 & 2

NICE Framework Users Group 6th floor, Chastain D & E

Apprenticeships in Cybersecurity 6th floor, Chastain F & G

Cybersecurity Skills Competition 6th floor, Chastain H,I,&J







EXHIBIT HALL BREAK

Augusta Ballroom, 7th Floor 2:15 p.m. – 3:00 p.m.

GIAC Technology Showcase: Fixing the Gap(s) in the Cyber Workforce







BREAKOUT SESSIONS

3:00 p.m. - 3:45 p.m.

Investigating Disparities in K12 Cybersecurity Education: Case Study and Approaches 6th floor, Chastain 1 & 2

Defining Diversity within Cybersecurity within the Spectrum of Career Categories 6th floor, Chastain D & E

CASCADE Apprenticeship Programs and Cyber Career Map 6th floor, Chastain F & G

Emerging Tech Cybersecurity Myth Smackdown: Perspectives from the Field 6th floor, Chastain H,I,&J

FIORIDA INTERNATIONAI UNIVERSITY





BREAK

3:45 p.m. – 4:00 p.m.







INFORMATION OPERATIONS ARE A CYBERSECURITY PROBLEM: TOWARD A NEW STRATEGIC PARADIGM TO COMBAT DISINFORMATION

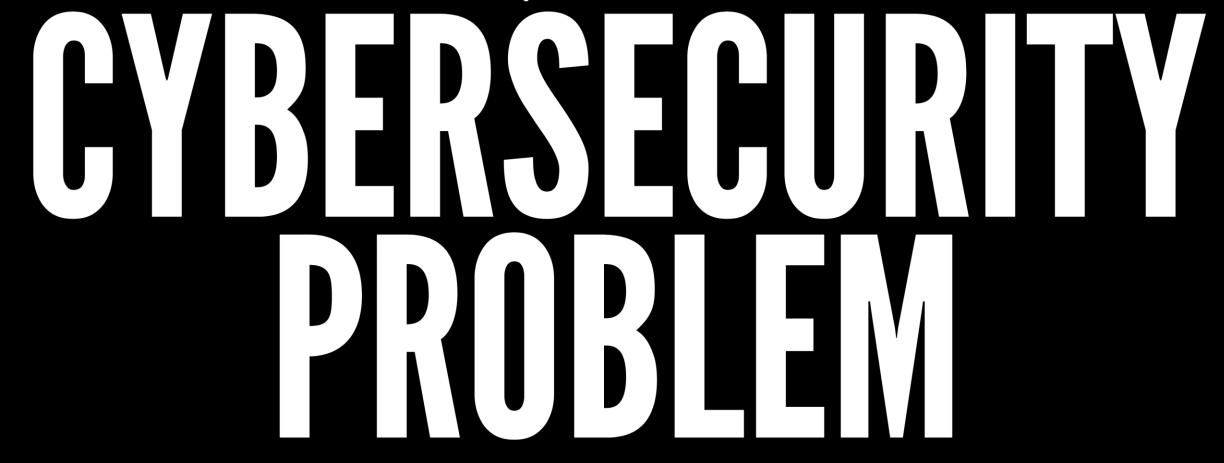
Renee DiResta

Research Manager Stanford University





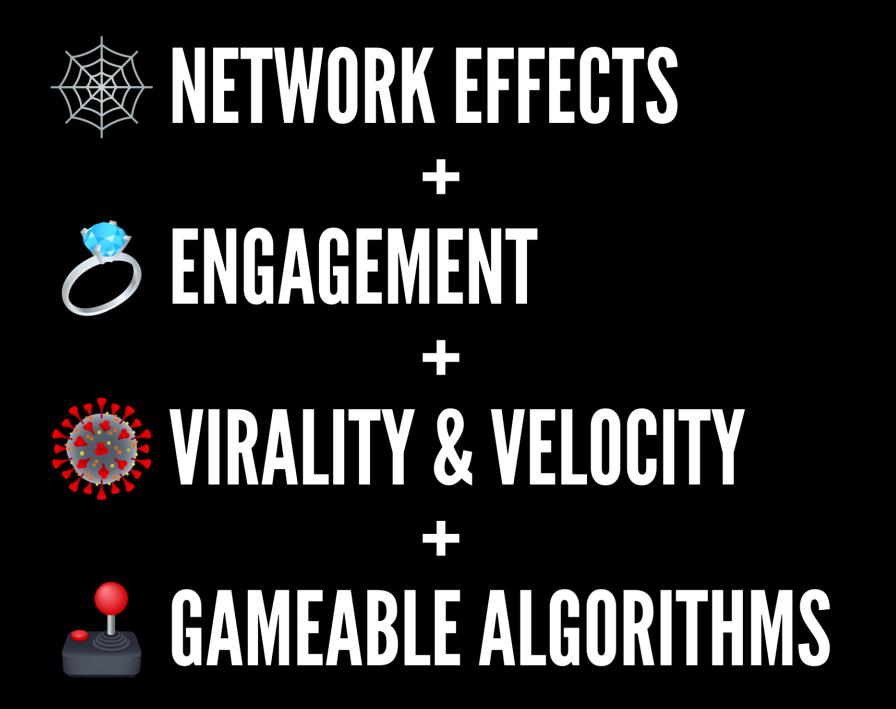
Disinformation as a

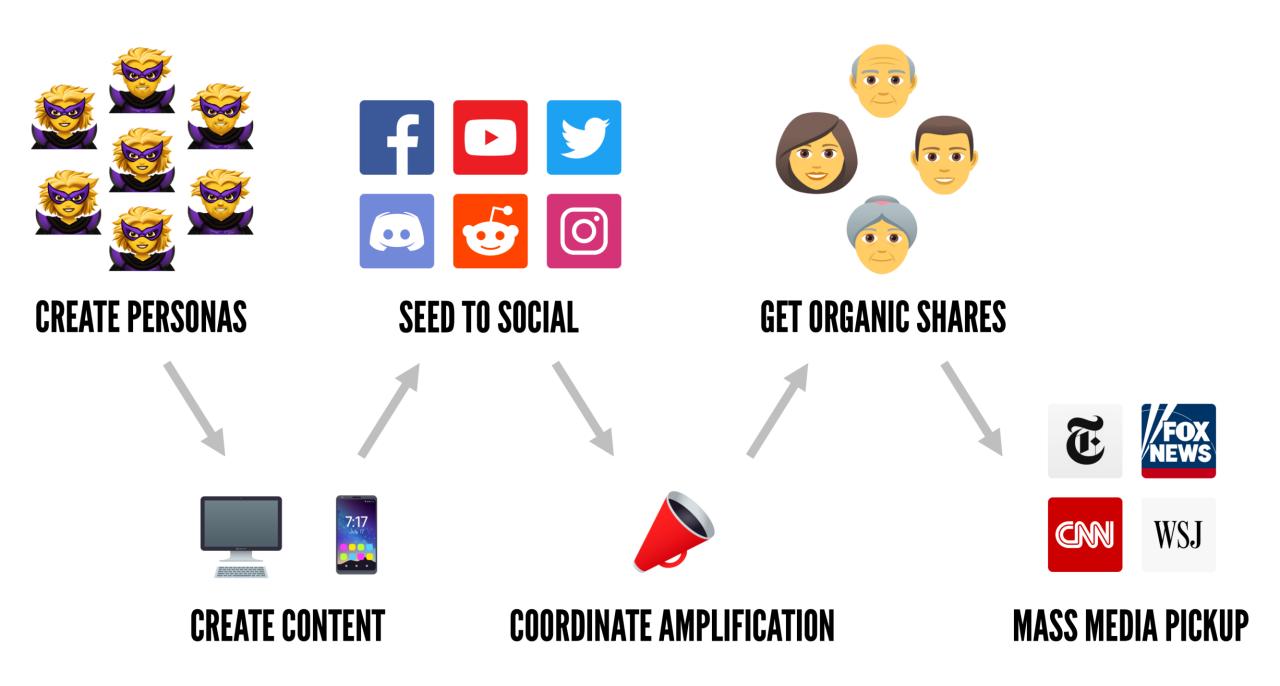


@noUPSIDE RENEE DIRESTA



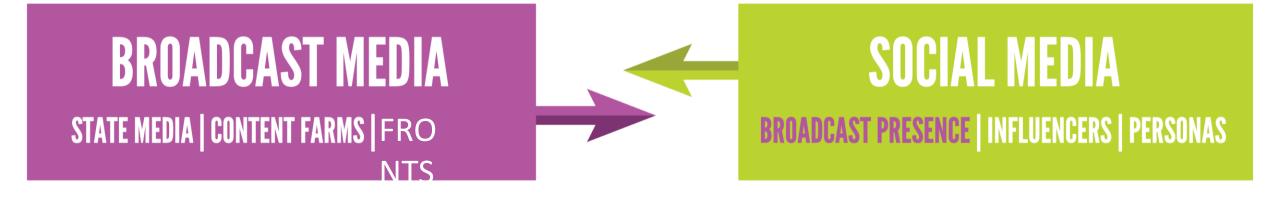








INFLUENCE OPERATIONS ADAPT TO FIT THE INFORMATION ENVIRONMENT OF THE DAY.





Philip Lyndon @PhilipLyndon2

My gay friend who lives in **#Ukraine** sent me this. I'm sure it is not ok that same-sex couples are not allowed to have kids and still have to pay those taxes for families w/o children. That's ridiculous.







17 Feb, 2022 17:42 / Home / Russia & FSU

...

Russia tells NATO to 'calm down' over Ukraine

Western officials need to tone down 'hysteria' over an invasion, the Deputy Foreign Minister said

By Ailis Halligan

Аналитик Подоляка рассказал о массовом побеге украинских политиков из страны

13 февраля 2022 21:07

политика



Russian Embassy, UK @RussianEmbassy P Russia government organization

FM #Lavrov on the #Mariupol attack: The maternity house was long non-operational. Instead, it was used by marmed forces and radicals, namely the neo-Nazi Azov Battalion. Moreover, #Russia warned #UN Security Council about this 3 days ago.



💄 MFA Russia 💼 and 9 others

1:31 PM · Mar 10, 2022 · Twitter Web App



...

Russian Embassy, UK 🤣 @RussianEmbassy M Russia government organization

Replying to @XSovietNews @mfa_russia and 9 others

No, it's the indeed pregnant beauty blogger Marianna Podgurskaya. She actually played roles of both pregnant women on the photos. And first photos were actually taken by famous propagandist photographer Evgeniy Maloletka, rather than rescuers and witnesses as one would expect.



1:42 PM · Mar 10, 2022 · Twitter Web App



WarOnFakes.com

Armed Forces of Ukraine

Civilians

(Donetsk People's Republic)

DPR

(Lugansk People's Republic)

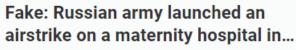
LPR

The Russian Federation

Ministry of Defense

Our Telegram 1 channel





The Russian Federation Ministry of Defense 02.04.2022 12:40 Russian army launched an airstrike on a maternity hospital in Mariupol. Back in March, this news was at the

Fake: Russian Army are shelling residential areas in Mariupol

The Russian Federation Ministry of Defense 01.04.2022 10:34

The Russian Army are shelling residential areas in Mariupol and filming their own crimes on video.

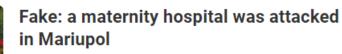
Fake : Russia bombed the drama theater with civilians in Mariupol раматический театр, в бомбоубежище



Civilians 24.03.2022 16:59

top...

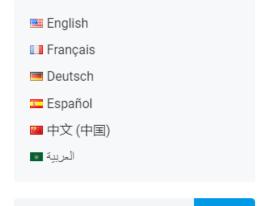
Ukrainian Defense Minister Oleksiy Reznikov says Russia is seeking to destroy his country.



Civilians 18.03.2022 17:58

1 0 4 Maut

Vladimir Zelensky has repeatedly mentioned that a maternity hospital was attacked in Mariupol. In his another address President Zelensky said...



4 Manifest 4

mariupol

Welcome to the "War on Fakes" project. We are the owners and administrators of several Russian non-political telegram channels.

Search

We don't do politics. But we consider it important to provide unbiased information about what is happening in Ukraine and on the territories of Donbass, because we see signs of an information war launched against Russia.

Our mission is to make sure that there are only objective publications in the information space.

We do not want ordinary people to feel anxious and panicked because of information wars.

We are going to look into every fake and give links to the real refutations. Be safe, be at peace, be with us.



Мариуполе разбомбили

торого прятались люди

EU to ban Russian state-backed channels RT and Sputnik

Ursula von der Leyen says stations will 'no longer be able to spread their lies to justify Putin's war'

Russia-Ukraine war latest news: follow live updates



Still from RT coverage of Ukraine invasion. Photograph: RT News

The EU has announced it will ban the Russian state-backed channels **RT** and Sputnik in an unprecedented move against the Kremlin media machine.

Known persistent threat actors

First, following our last security update on Ukraine, we've seen a further spike in compromise attempts aimed at members of the Ukrainian military by Ghostwriter, a threat actor <u>tracked</u> by the security community. As we've <u>shared</u> before, Ghostwriter typically targets people through email compromise and then uses that to gain access to their social media accounts across the internet. Since our last public <u>update</u>, this group has attempted to hack into the Facebook accounts of dozens of Ukrainian military personnel. In a handful of cases, they posted videos calling on the Army to surrender as if these posts were coming from the legitimate account owners. We blocked these videos from being shared.

Second, we detected and took down an attempt to come back by a network we removed in December 2020 and linked to individuals associated with past activity by the Russian Internet Research Agency (IRA). Their off-platform activity appears to have begun last year and centered around a website, posing as an NGO focused on civil rights in the West. They unsuccessfully attempted to create Facebook accounts in late 2021 and January 2022. Throughout January and February of this year, the website published about police violence in the West, but since the invasion, their articles blamed Russia's attack on NATO and the West and accused Ukrainian forces of targeting civilians.

Politically-aligned non-state actors

We detected and took down an attempt to come back by the network we removed in <u>December</u> <u>2020</u> and linked to people in the Luhansk region of Ukraine. This activity centered around two websites promoting pro-Russian commentary in the Caucasus and Ukraine, and a small number of accounts on Facebook, Telegram, VK, and OK. In early March, the Ukraine-focused site appeared to have been taken over to direct its audience towards a Telegram channel showing photos of Russian casualties.

We also removed a network in Russia for violating our Inauthentic Behavior policy against mass reporting. The network coordinated to falsely report people in Ukraine and also in Russia for various violations, including hate speech, in an attempt to have them and their posts removed from Facebook. More details on this network can be found <u>here</u>.



17 Mar, 2022 19:30 / Home / Russia & FSU

Russia presents new evidence from USfunded Ukraine biolabs

Pentagon-backed facilities made "biological weapons components" and tried to cover it up, Russian military says



Russian Embassy, UK @ @RussianEmbassy · Mar 7

#Lavrov: While categorically refusing to establish a verification mechanism in keeping with Biological Weapons Convention, #US built military biol. facilities along border. Now is worried about losing control of those in , incl 2 labs in #Kiev & #Odessa creating pathogens.



MFA Russia 🚃 and 9 others



Published March 14, 2022 11:29am EDT

Tucker: The Pentagon is lying about bio labs in Ukraine

How 'Ukrainian bioweapons labs' myth went from QAnon fringe to Fox News

A feedback loop involving Russia and Tucker Carlson is promoting claims of US funding for biological weapons in Ukraine





China government official

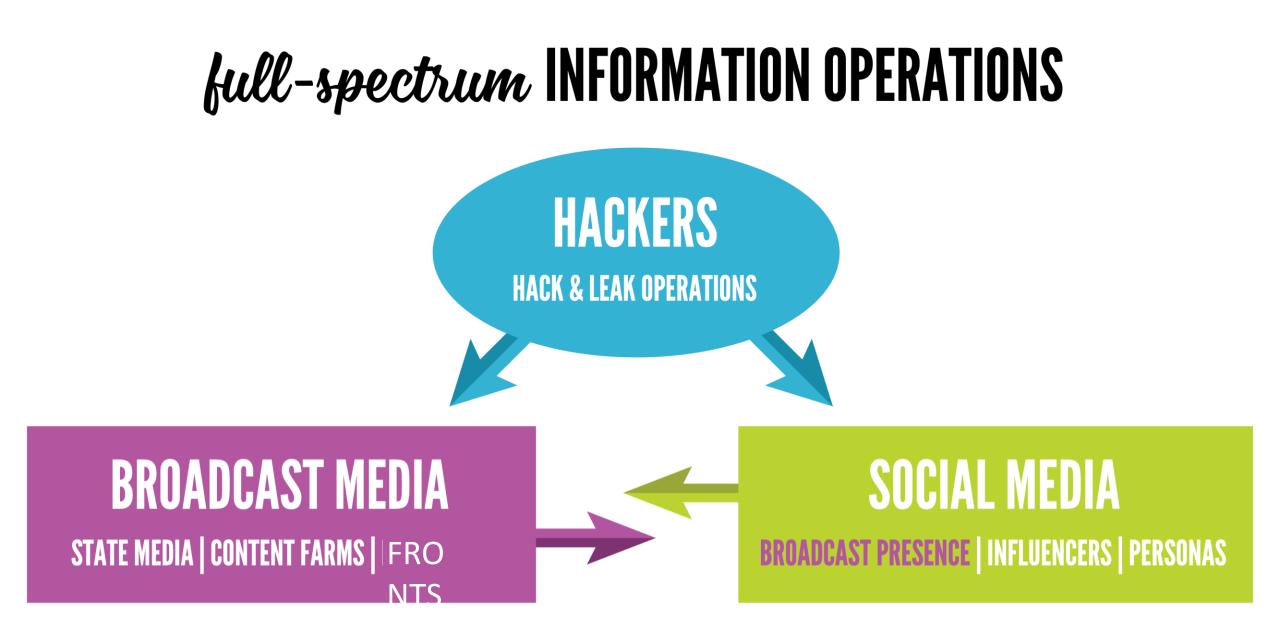
The US bio-military activities are not transparent, safe or justified. In Ukraine alone, the US has set up 16 biolabs. Why does the US need so many labs all over the world? What activities are carried out in those labs, including the one in Fort Detrick?



10:05 AM - Apr 8, 2021 - Twitter Web App

498 Retweets 141 Quote Tweets 1.810 Likes

MALIGN ACTORS EXPLOIT **DIVISIONS IN OUR SOCIETY USING VULNERABILITIES IN OUR INFORMATION ECOSYSTEM.**



"Very English Coop d'Etat"

It's the most horrifying conspiracy-fact in the latest British history we are going to tell you about. What would you say if they tell you that the country you live in is governed by the coup plotters? That these hoaxers control their puppet - sneaky strawhead?

But that's not the whole story. Can you just imagine that ex-MI6 Chief together with his former colleagues and CIA cronies conducted successful intelligence operation against No 10? To pave the way for their puppet they penetrated No 10 with the secret agent inside the Civil Service to steal highly sensitive documents and blackmailed the then Prime Minister. These plotters colluded with American media tycoons to intervene just before the Vote in Parliament. They targeted senior Civil Servants and forced them to resign. In addition, many acting Government officials were part of the conspiracy.

And moreover. These crazy people believe in "deep state", "evil Soros" and disseminated pictures of the then Prime Minister as a Harry Potter Dementor.

Still can't believe? Keep calm and read this bunch of the most amazing secret emails you have ever seen.



Gisela Stuart, Baroness Stuart of Edgbaston

Freedly also had a standard a second

Sir Richard Dearlove, KCMG OBE Head of the British Secret Intelligence Service (MI6) from 1999 until 6 May 2004, a role known informally as "C" Robert Gascoyne-Cecil, 7th Marquess of Salisbury, Baron Gascoyne-Cecil, KG, KCVO, PC, DL

British Conservative politician



5 Jun, 2022 16:12 / Home / World News

Massive leak alleges deep-state Brexit conspiracy

Those implicated by the publication downplayed it as 'legitimate lobbying' and dismissed it as Russian 'disinformation' at the same time



FILE PHOTO. © Getty Images / Loredana Sangiuliano / SOPA Images / LightRocket

An elaborate high-profile conspiracy allegedly run by shadowy figures within the British elite was exposed in a massive leak released by a group of hackers late in May. The cache of documents and emails alleging a deep-state plot by hardcore Leavers to deliver the 'hardest' Brexit possible is now available on the website 'Very English Coop d'Etat'.

Plotting for a hard Brexit

The conspiracy involved the most hardcore Leavers: Former head of MI6 Richard Dearlove, former NATO and Defence Ministry adviser Gwythian Prins, leading Brexit campaigner and ex-Labour MP Baroness Stuart, professor emeritus of French history at the University of Cambridge Robert Toombs, and others.

The goals of the campaign, dubbed 'Operation Surprise', were outlined in a 2018 document penned by Prins, who proclaimed the need to *"take the fight to our opponents, who are remorseless, by all necessary means."* The plotters sought to deliver the 'hardest' Brexit possible, targeting both those seeking to continue the UK's membership in the EU, and proponents of 'soft' Brexit alike.

RENEE DIRESTA @noUPSIDE

NICE Conference and Expo 2022

JUNE 6 - 8, 2022 | WESTIN PEACHTREE PLAZA | ATLANTA, GA

DEMYSTIFYING CYBERSECURITY

Integrated Approaches to Developing Career Pathways







EVENING RECEPTION

Augusta Ballroom, 7th Floor 5:00 p.m. – 6:00 p.m.





#NICECYBERCON22