

PSCI/PPPE 6302
Political Violence and Conflict in Cyberspace
FALL 2020

Instructor: Vito D’Orazio

Time and Location: Thursday 7:00-9:45pm

Modality: Remote, Synchronous

Email: dorazio@utdallas.edu

Office: GR 3.108D

Office Phone: 972-883-6212

Office Hours: Individual or group meetings on MS Teams available by appointment.

Course Modality and Expectations

Instructional Mode The instructional mode is *remote*. This means “synchronous online learning at the day and time of the class. The instructor delivers the instruction from home or the office. Students complete the course at a distance.” See <https://www.utdallas.edu/fall-2020/fall-2020-registration-information/> for more information.

Course Platform The class will meet at our scheduled time on MS Teams. Students can join and view meeting details by selecting the Calendar tab on Teams. For group projects, students will meet on MS Teams at a mutually agreeable time.

Expectations Students who do not choose the asynchronous option are expected to attend class at our regularly scheduled time and to participate as if the class were in-person. Class discussion is a critical part of graduate learning, so all students are expected to complete the weekly assignments and come to class prepared to discuss.

Asynchronous Learning Guidelines Students may select the asynchronous option at any time. Students who select the asynchronous option must notify the instructor. For each week that the student is engaged in asynchronous learning, the student is required to complete the asynchronous assignment, described below in the Attendance and Participation section.

For more information on asynchronous learning: <https://www.utdallas.edu/fall-2020/asynchronous-access-for-fall-2020/>

COVID-19 Guidelines and Resources

The information contained in the following link lists the University's COVID-19 resources for students and instructors of record.

Please see <http://go.utdallas.edu/syllabus-policies>.

Course Description

This course examines the role of cyberspace, or the cyber domain, in international and domestic politics. It has a specific emphasis on foreign policy, political violence, democratization, autocratization, repression, and protest.

What is cyberspace? According to the US Department of Defense:

Cyberspace consists of many different and often overlapping networks, as well as the nodes (any device or logical location with an Internet protocol address or other analogous identifier) on those networks, and the system data (such as routing tables) that support them. Cyberspace can be described in terms of three layers: physical network, logical network, and cyber-persona. The physical network layer of cyberspace is comprised of the geographic component and the physical network components. It is the medium where the data travel. The logical network layer consists of those elements of the network that are related to one another in a way that is abstracted from the physical network, i.e., the form or relationships are not tied to an individual, specific path, or node. A simple example is any Web site that is hosted on servers in multiple physical locations where all content can be accessed through a single uniform resource locator. The cyber-persona layer represents yet a higher level of abstraction of the logical network in cyberspace; it uses the rules that apply in the logical network layer to develop a digital representation of an individual or entity identity in cyberspace. The cyber-persona layer consists of the people actually on the network.

Van Puyvelde and Brantly (2019), which is our introduction to the field, find utility in this DoD definition of cyberspace, and we'll use it throughout the semester. While this definition is extensive and there is no expectation that students fully grasp it yet, one thing is clear: cyberspace is vast. It includes all your smart and connected devices (e.g. cell phones, thermostats, Ring, cars, televisions), all of social media (e.g., Twitter, Instagram, Facebook, Tik Tok), the World Wide Web and its billions of pages, intranets, anything connected to the Internet in any way, shape, or form, ... you get the idea.

Throughout this course, we will explore the ways that cyberspace affects international and domestic politics. The first section will focus primarily on the international domain. We will study classic international relations topics such as power, the security dilemma, and the offense-defence balance in cyberspace. We will also examine the ways that states have used cyberspace to pursue their foreign policy interests, using specific examples such as Stuxnet.

The second section will shift to domestic politics and explore topics that are typically at the intersection of international relations and comparative politics (sub-fields of Political Science). We will study the way cyberspace is used for repression and autocratization, as well as social protest and democratization. We will also study the way the Internet and the cyber domain (which includes the Internet) has affected violent conflicts in Africa, Asia, and elsewhere. We will discuss topics such as the strategic use of blackouts during times of political instability, and the role of social media in the Arab Spring.

As Bruce Schneier writes in *Click Here to Kill Everybody*, “everything is becoming a computer.” As more things become computers, the already vast cyberspace expands, and there’s no telling where it will end. If we want to understand politics and security in the 21st Century, we need to understand the role of this behemoth of a thing called cyberspace.

Learning Objectives

There are three learning objectives for this course. The first is for students to understand the above definition of cyberspace, in all its complexities. This includes a detailed understanding of its origins, what it entails currently, and what cyberspace may look like in the future. The second learning objective is for students to develop a catalog of important political and societal events that have prominently featured activity in cyberspace. In addition to the details of particular events, the objective is for students to understand the context in which the event took place along with its implications. The third learning objective is for students to understand, apply, compare, evaluate, and synthesize existing theories pertaining to the role of cyberspace in international and domestic politics. These three learning objectives will be assessed through class discussion, homework assignments, group presentations, and the final project.

Course Requirements

There will be about four articles or one book assigned per week. Students are expected to read each in detail and to be prepared to discuss. I will begin each class with prepared comments on the readings that are designed (1) to provide some additional context and organization of major themes, and (2) to bring forth important issues that I see in this set of readings. While I will lead the discussion, this is not a lecture. I expect meaningful contributions from each student.

Final Grade Composition

Attendance and participation	20%
Homework assignments	30%
Final project	30%
Group presentations	20%

Attendance and Participation (20%)

For synchronous students, 20% of the grade depends on participation in class discussions, and attendance and participation in the group meetings. Students are expected to show up on time, be attentive, and engage the class discussion. Please come to class having read the material and prepared to discuss.

Our classes will meet virtually for two hours, from 7-9pm. The additional 45 minutes of class time will be shifted to group meetings at a time to be determined by each group. The selected time should also accommodate our asynchronous students, who are required to attend the group meetings. Each week, one member from each group is to complete and upload the Group Meeting Form (available on eLearning), to their group's channel on Teams.

For asynchronous students, or for any week where the asynchronous option is selected, participation will be assessed with the asynchronous assignment (in addition to participation in group meetings). Asynchronous students are expected to submit a reading review (#1-3), which is due before class, and a post-discussion follow-up (#4), which is due prior to the following week's class. For the reading review:

1. Summarize the reading (1 paragraph)
 - Keep this concise, but be sure to summarize the entire reading list for the week and not just part of it. For example, summarize the entire book or all articles. You may summarize each article, or sections of a book, independently, rather than attempting to synthesize the readings.
2. Raise two thoughtful questions
 - These should not be straightforward “yes or no” type questions. Instead, try to raise “why” and “how” questions. The difference is often subtle, but can encourage you to think about the underlying processes. For example, instead of asking *whether* Stuxnet was a successful cyber attack, ask *how* was Stuxnet a success and how was it a failure. What are some ways that Stuxnet changed how states pursue foreign policy?
3. Discuss your reaction to the reading (1-2 paragraphs)
 - The reaction (or response) should demonstrate elements of comparison, evaluation, synthesis, or creativity. You should feel free to write about anything related to the reading, and not limit yourself to only the reading itself. For example, incorporate current events, other readings from this class or other classes, or things that you've discussed in this class or elsewhere. You might consider how the author's argument compares with that of others. Or, whether you agree with the authors argument and why? Can you provide cases that the theory does not support? For example, if the author is arguing that uncertainty is a cause of conflict escalation and that uncertainty increases in cyberspace, can you think of cases where uncertainty actually decreased in cyberspace? If so, then perhaps the

author's assumption about cyberspace and uncertainty is incorrect. Feel free to get creative with your reaction.

4. Post-discussion follow-up

- The post-discussion follow-up is essentially an assessment of your assignment based on the class discussion. Go through each section of your submission—summary, questions, response—and assess your work using the recorded discussion. Did the summary miss a key point? Or over-emphasize a lesser point? Were your questions answered? Or, do you have new questions that you'd like answered? In what ways did the discussion impact your response?

The asynchronous assignment is to be submitted on eLearning.

Homework assignments (30%)

Each homework assignment is worth 10 points. All students must complete three of the four assignments. If you choose to complete all four, the lowest grade will be dropped. If for any reason you cannot complete the assignment, you must notify me before the assignment is due and we can make arrangements to complete the work. Students are required to submit assignments through eLearning by the start of class on the day the assignment is due.

For each assignment, students will write a literature review that is three to five pages in length, excluding the references. The literature review should have a clear research question and should progress toward one or more explicitly stated hypotheses. The hypotheses do not need to be entirely new or novel, but they should flow logically from your review of the existing literature. The literature review must have a minimum of 10 new citations from articles that were not assigned readings.

Additional details and guidance for these assignments will be provided by the instructor.

Group Presentations (20%)

Each group presentation is worth 10 points. The presentation is a case study designed to help to construct a catalog of important political and societal events that have prominently featured activity in the cyber domain. Each group is to select one such event and construct a presentation for the class on the event. With a focus on the cyber component, the presentation should identify the who, what, where, when, why, and how. It should discuss the relevant events that led up to the event, the context in which it happened, and the results along with any broader significance. Groups should think of this as a lesson for the class, and shape their presentation accordingly.

Each group is required to notify the instructor of the topic of the presentation once it has been decided. The storyboxes in Van Puyvelde and Brantly might be helpful for choosing events. Note how they are not overly specific, and tend to focus on higher-level events. For example, Storybox 5.1 is *Russian Interference* and Storybox 6.2 is *Ukrainian Blackouts*. This is about the level of specificity that you should plan to present on.

I encourage you to be creative with your presentation. Your group may do it live, or you may record it in advance. You may deliver a standard presentation from a slide deck, or you might opt for something different. For example, enact a scripted debate or deliver a news segment. You can make something with a social media platform, or in the style of something that would appear on a social media platform. I will assess the presentation for content using the above criteria, but how that content is communicated is up to you.

Groups will be assigned by the instructor, and will be different for each assignment. Each group will be given a private channel on Teams to coordinate and discuss. Students are expected to meet for forty-five minutes at a mutually agreeable time. Feel free to invite the instructor to attend! Note that our regular class meetings will last for two hours, not two hours and forty-five minutes, so these meetings are intended to comprise that additional class time. Following the weekly meeting, a group member is to complete the Group Meeting Form (available on eLearning) and upload it to their group's channel on Teams.

Asynchronous students are expected to attend the group meetings at the mutually agreeable time. If this is not possible, please let the instructor know in advance so we can make arrangements.

Final Project (30%)

The final project is anything that may be described as a *research product*. This includes a paper for a peer-reviewed journal, a blog (e.g., see The Monkey Cage at the *Washington Post*), a white paper, a think-tank policy piece, a newspaper op-ed, a conference presentation (a professional slide deck for a 15 minute presentation), a poster-board (UTD has templates: <https://utdallas.app.box.com/s/4a7viyes14quwhs5ns7f9xac57s8ggg6>), a web site, a piece of software, a dataset, a lecture, whatever. Be creative. This class has many students from diverse backgrounds and who wish to achieve different goals. Select a research product that best fits your objectives.

All students must clear their research project with the instructor and, prior to beginning, **provide the instructor with a research project proposal**. The proposal should indicate the type of product you will create, the topic, and will include an example to emulate. For example, if you select a peer-reviewed journal article, provide a quality example that you believe is most similar to the type of article you wish to write. If a poster-board, find an example on the Web from a professional conference.

Final papers are due by midnight on Friday, December 4.

Grade Scale

A	≥ 93%	B	= 83-86%	C	73-76%
A-	= 90-92%	B-	= 80-82%	F	≤ 72%
B+	= 87-89%	C+	= 77-79%		

See <https://catalog.utdallas.edu/2020/graduate/policies> for additional information about university grading policies.

Required Texts

Several of these texts are available online through the UT Dallas library: <https://www.utdallas.edu/library/>

- Buchanan, B. (2017). *The Cybersecurity dilemma: Hacking, trust and fear between nations*. Oxford University Press. ISBN: 978-0190665012
- Kreps, S. (2020). *Social Media and International Relations*. Elements in International Relations. Cambridge University Press
 - PDF made available by instructor
- Roberts, M. E. (2018). *Censored: distraction and diversion inside China's Great Firewall*. Princeton University Press. ISBN-13: 978-0-691-20400-0
- Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press. ISBN-13: 978-0-300-21512-0
- Valeriano, B., Jensen, B. M., and Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion*. Oxford University Press. ISBN-13: 978-0-19-061809-4
- Van Puyvelde, D. and Brantly, A. F. (2019). *Cybersecurity: politics, governance and conflict in cyberspace*. Polity. ISBN-13: 978-1-5095-2809-7
- Weidmann, N. B. and Rød, E. G. (2019). *The Internet and political protest in autocracies*. Oxford Studies in Digital Polics. ISBN-13: 978-0190918316
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books. ISBN-13: 978-1-5417-5800-1

Additional Texts

- Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press. ISBN-13: 978-0674987555
- Abbate, J. (2000). *Inventing the internet*. MIT press. ISBN-13: 978-0262511155

Course Outline

Day 1: Introductions, Syllabus, and Cyber Domain

August 20

- Week 1 assignment due

The (Mostly) International Cyber Domain

Day 2: Cybersecurity

August 27

- Van Puyvelde, D. and Brantly, A. F. (2019). *Cybersecurity: politics, governance and conflict in cyberspace*. Polity. ISBN-13: 978-1-5095-2809-7

Day 3: Cyberspace

September 3

- Nye Jr, J. S. (2010). Cyber power. Technical report, Harvard University Belfer Center for Science and International Affairs. <https://apps.dtic.mil/dtic/tr/fulltext/u2/a522626.pdf>
- Gartzke, E. (2013). The myth of cyberwar: bringing war in cyberspace back down to earth. *International Security*, 38(2):41–73
- Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, 22(3):365–404

Day 4: Cybersecurity Dilemma

September 10

*Homework #1 due

- Buchanan, B. (2017). *The Cybersecurity dilemma: Hacking, trust and fear between nations*. Oxford University Press. ISBN: 978-0190665012

Day 5: Cyber Escalations

September 17

- Slayton, R. (2017). What is the cyber offense-defense balance? conceptions, causes, and assessment. *International Security*, 41(3):72–109
- Gartzke, E. and Lindsay, J. R. (2017). Thermonuclear cyberwar. *Journal of cybersecurity*, 3(1):37–48
- Kreps, S. and Schneider, J. (2019). Escalation firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics. *Journal of Cybersecurity*, 5(1):tyz007

Day 6: Cyber Strategy

September 24

*Homework #2 due

- Valeriano, B., Jensen, B. M., and Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion*. Oxford University Press. ISBN-13: 978-0-19-061809-4

Day 7: Project Presentations #1

October 1

- Group project #1

The (Mostly) Domestic Cyber Domain

Day 8: Domestic Cyber Domain

October 8

- Gohdes, A. R. (2018). Studying the internet and violent conflict. *Conflict Management and Peace Science*, 35(1):89–106
- Gohdes, A. R. (2015). Pulling the plug: Network disruptions and violence in civil conflict. *Journal of Peace Research*, 52(3):352–367
- Gohdes, A. R. (2020). Repression technology: Internet accessibility and state violence. *American Journal of Political Science*
- Pierskalla, J. H. and Hollenbach, F. M. (2013). Technology and collective action: The effect of cell phone coverage on political violence in africa. *American Political Science Review*, 107(2):207–224

Day 9: Social Media

October 15

- Kreps, S. (2020). *Social Media and International Relations*. Elements in International Relations. Cambridge University Press
- Cleaver Jr, H. M. (1998). The zapatista effect: The internet and the rise of an alternative political fabric. *Journal of International Affairs*, pages 621–640

Day 10: Twitter Revolution

October 22

*Homework #3 due

- Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press. ISBN-13: 978-0-300-21512-0
- Morozov, E. (2009). Iran: Downside to the” twitter revolution”. *Dissent*, 56(4):10–14

Day 11: The Internet and Political Protest

October 29

- Weidmann, N. B. and Rød, E. G. (2019). *The Internet and political protest in autocracies*. Oxford Studies in Digital Polics. ISBN-13: 978-0190918316

Day 12: Internet in China I

November 5

*Homework #4 due

- Roberts, M. E. (2018). *Censored: distraction and diversion inside China’s Great Firewall*. Princeton University Press. ISBN-13: 978-0-691-20400-0

Day 13: Internet in China II**November 12**

- King, G., Pan, J., and Roberts, M. E. (2013). How censorship in china allows government criticism but silences collective expression. *American Political Science Review*, 107(2):326–343
- King, G., Pan, J., and Roberts, M. E. (2017). How the chinese government fabricates social media posts for strategic distraction, not engaged argument. *American Political Science Review*, 111(3):484–501

Day 14: Project Presentations #2**November 19**

- Group project #2

***Final projects are due by midnight on Friday, December 4.**

Class Participation

Regular class participation is expected regardless of course modality. Students who fail to participate in class regularly are inviting scholastic difficulty. A portion of the grade for this course is directly tied to your participation in this class. It also includes engaging in group or other activities during class that solicit your feedback on homework assignments, readings, or materials covered in the lectures (and/or labs). Class participation is documented by faculty. Successful participation is defined as consistently adhering to University requirements, as presented in this syllabus. Failure to comply with these University requirements is a violation of the Student Code of Conduct: <https://policy.utdallas.edu/utdsp5003>.

Class Recordings

Students are expected to follow appropriate University policies and maintain the security of passwords used to access recorded lectures. Unless the Office of Student AccessAbility has approved the student to record the instruction, students are expressly prohibited from recording any part of this course. Recordings may not be published, reproduced, or shared with those not in the class, or uploaded to other online environments except to implement an approved Office of Student AccessAbility accommodation. Failure to comply with these University requirements is a violation of the Student Code of Conduct: <https://policy.utdallas.edu/utdsp5003>.

The instructor may record meetings of this course. Any recordings will be available to all students registered for this class as they are intended to supplement the classroom experience. Students are expected to follow appropriate University policies and maintain the security of passwords used to access recorded lectures. Unless the Office of Student AccessAbility has approved the student to record the instruction, students are expressly prohibited from recording any part of this course. Recordings may not be published, reproduced, or shared with those not in the class, or uploaded to other online environments except to implement an approved Office of Student AccessAbility accommodation. If the instructor or a UTD school/department/office plans any other uses for the recordings, consent of the students identifiable in the recordings is required prior to such use unless an exception is allowed by law. Failure to comply with these University requirements is a violation of the Student Code of Conduct: <https://policy.utdallas.edu/utdsp5003>.

Class Materials

The Instructor may provide class materials that will be made available to all students registered for this class as they are intended to supplement the classroom experience. These materials may be downloaded during the course, however, these materials are for registered students' use only. Classroom materials may not be reproduced or shared with those not in class, or uploaded to other online environments except to implement an approved Office of Student AccessAbility accommodation. Failure to comply with these University requirements is a violation of the Student Code of Conduct: <https://policy.utdallas.edu/utdsp5003>.

Additional Information and Resources

Technical Requirements

In addition to a confident level of computer and Internet literacy, certain minimum technical requirements must be met to enable a successful learning experience. Please review the important technical requirements on the Getting Started with eLearning webpage: <https://ets.utdallas.edu/elearning/students/current/getting-started>.

Course Access and Navigation

This course can be accessed using your UT Dallas NetID account on the eLearning website: [elearning.utdallas.edu](https://ets.utdallas.edu).

Please see the course access and navigation section of the Getting Started with eLearning webpage for more information: <https://ets.utdallas.edu/elearning/students/current/getting-started>.

To become familiar with the eLearning tool, please see the Student eLearning Tutorials webpage: <https://ets.utdallas.edu/elearning/students/current/tutorials>

UT Dallas provides eLearning technical support 24 hours a day, 7 days a week. The eLearning Support Center includes a toll-free telephone number for immediate assistance (1-866-588-3192), email request service, and an online chat service: <https://ets.utdallas.edu/elearning/helpdesk>.

Communication

This course utilizes online tools for interaction and communication. Some external communication tools such as regular email and a web conferencing tool may also be used during the semester. For more details, please visit the Student eLearning Tutorials webpage for video demonstrations on eLearning tools: <https://ets.utdallas.edu/elearning/students/current/tutorials>.

Student emails and discussion board messages will be answered within 3 working days under normal circumstances.

Distance Learning Student Resources

Online students have access to resources including the McDermott Library, Academic Advising, The Office of Student AccessAbility, and many others. Please see the eLearning Current Students webpage for more information: <https://ets.utdallas.edu/elearning/students/current>.

Server Unavailability or Other Technical Difficulties

The University is committed to providing a reliable learning management system to all users. However, in the event of any unexpected server outage or any unusual technical difficulty

which prevents students from completing a time sensitive assessment activity, the instructor will provide an appropriate accommodation based on the situation. Students should immediately report any problems to the instructor and also contact the online eLearning Help Desk. The instructor and the eLearning Help Desk will work with the student to resolve any issues at the earliest possible time: <https://ets.utdallas.edu/elearning/helpdesk>.

Comet Creed

This creed was voted on by the UT Dallas student body in 2014. It is a standard that Comets choose to live by and encourage others to do the same:

“As a Comet, I pledge honesty, integrity, and service in all that I do.”

Academic Support Resources

The information contained in the following link lists the University’s academic support resources for all students.

Please go to Academic Support Resources webpage for these policies: <https://provost.utdallas.edu/syllabus-policies/#academic-support-resources>

UT Dallas Syllabus Policies and Procedures

The information contained in the following link constitutes the University’s policies and procedures segment of the course syllabus.

Please go to UT Dallas Syllabus Policies webpage for these policies: <https://go.utdallas.edu/syllabus-policies>.

The descriptions and timelines contained in this syllabus are subject to change at the discretion of the Professor.