13th Annual Clara Barton Competition, 2026
Saturday, March 14

CLARA BARTON
INTERNATIONAL HUMANITARIAN LAW COMPETITION

Round 3

Prep Window:
Wave A: 1:30-2:30pm
Wave B: 2:30-3:30pm

Test Window:
Wave A: 2:35-3:00pm
Wave B: 3:35-4:00pm

Roles:	Burcet Department of State Legal Advisors	Burcet Department of Defense Legal Advisors
Teams:	1,2,5,6,9,10,13,14	3,4,7,8,11,12,15,16

Room Assignments:	17-BoG	17-G08	18-202	18-215
Wave A Teams:	2,4	6,8	5,7	1,3
Wave B Teams:	10,12	14,16	13,15	9,11

Immediately after the round concludes, there will be a 10-minute window for judge feedback in the same room.

Delete Archive Report

Operation Northern Shield - Cyber Operation Options

ME

Mary Todd Escola <mte@gov.bur>
To: awops7@dod.bur; legalint@dos.bur;

Saturday 03/14/2026 12:44 PM

Hi all,

Today's meeting is of the utmost importance to our next steps in our ongoing conflict with Stodia. As you know, the sheer geographic distance between our two nations pose substantial supply chain challenges. To counter this, the President has directed the military to propose options to degrade Stodia's warfighting capabilities via cyberspace. It now falls to the NSC – NS Working Group to consider the legal implications of the COAs detailed in the attached memorandum & supplemental information. To address this, please come to today's meeting prepared respectively to:

State: Advocate for VELVETSNARE and against THERMASPAN
Defense: Advocate for THERMASPAN and against VELVETSNARE

Your recommendations should include detailed legal analyses and proposed safeguards or conditions for authorization to ensure compliance with IHL. I've attached some relevant operational and context information as well as a helpful excerpt from our military manual.

See you soon,
Mary Todd,

Mary Todd Escola
Deputy General Counsel, Burcet National Security Council
Chair, Northern Shield Working Group

Reply Forward

BREAKING NEWS

Int. Press

SPECIAL EDITION

NAVAL SKIRMISHES AND AIRSPACE CLOSURES MARK OUTBREAK OF BURCET-STODIA CONFLICT

JANUARY 19, 2026

A long-simmering rivalry between the island nations of Burcet and Stodia erupted into open conflict early Monday morning, after a series of maritime and aerial incidents sharply escalated tensions across the Pale & Lerran Seas. Both governments confirmed that their armed forces were placed on full alert following what each side described as “unprovoked hostile actions” by the other.

The confrontation is the most serious clash between the two states in more than three decades and threatens to destabilize trade routes that link their respective territories and the continent of Forden, which lies between them.

How the Fighting Began

According to Burcet’s Department of Defense, the crisis began shortly after dawn on January 19, when Stodian naval patrol vessels allegedly entered Burcet’s claimed territorial waters. Burcet says its navy dispatched ships to escort the patrols away, leading to an exchange of warning shots and, later, limited live fire.

Stodia’s authorities rejected that account, stating that their vessels were conducting “routine freedom-of-navigation operations” and were intercepted aggressively by Burcetian forces. Stodia reported damage to at least one patrol craft and minor injuries among its crew.

By midday, both countries announced the closure of significant portions of their airspace, citing security concerns. Commercial airlines operating transcontinental routes over Forden reported widespread diversions, delays, and cancellations.

BREAKING NEWS

Int. Press

SPECIAL EDITION

Military Mobilization and Civilian Impact

Residents in Burcet's western port cities reported the sound of sirens and increased military traffic throughout the day. The government urged civilians to remain calm while advising fishing vessels and commercial shippers to avoid contested waters.

In Stodia, emergency sessions of the defense council resulted in the mobilization of reserve units and the reinforcement of coastal defenses. Public ferries between Stodia's fringe islands were temporarily suspended, leaving thousands of commuters stranded.

Humanitarian organizations expressed concern about the potential spillover effects, particularly if shipping disruptions lead to shortages of fuel and food imports, on which both island nations heavily depend.

Regional and International Reactions

Neighboring states across Forden issued statements calling for restraint, warning that even a limited conflict could have cascading economic effects. Several regional trade blocs urged immediate dialogue, while international observers offered to facilitate talks aimed at de-escalation.

Global markets reacted nervously, with shipping insurers raising premiums for vessels transiting the Novic Ocean. Energy analysts noted that while Burcet and Stodia are not major producers, the sea lanes affected by the conflict are critical conduits for fuel shipments.

What Comes Next

As night fell on January 19, reports emerged of sporadic radar lock-ons and continued naval maneuvering, though no large-scale engagements were confirmed.

For now, citizens in both Burcet and Stodia are bracing for uncertainty, as a rivalry shaped by geography and history, enters its most dangerous phase in a generation.

MEMORANDUM FOR THE NORTHERN SHIELD WORKING GROUP

FROM: JOINT CHIEFS OF STAFF, (STRATEGIC PLANS AND POLICY)
SUBJECT: Legal Review of Proposed Cyber Operations in Support of Operation NORTHERN SHIELD

1. Situation:
Burcet is engaged in an ongoing international armed conflict against the Stodia. Burcet's forces are conducting operations under the codename NORTHERN SHIELD. Stodia's military forces have proven to be a formidable adversary, leveraging advanced technology and a decentralized command and control (C2) structure. Burcet's Cyber Command has developed two potential courses of action (COAs) to disrupt Stodia's military operations.

2. Background:
Stodia's military relies heavily on the "Cerulean Grid," a network of interconnected data centers that host a variety of military and civilian services. The primary target of both proposed COAs is the "Azure Node," a key data center within the Cerulean Grid. The Azure Node is a dual-use facility: it hosts Stodia's military C2 servers, but also provides services to civilian and humanitarian organizations. (See EXH-CY-01: Azure Node Tenant List).

3. Proposed Courses of Action:
Two COAs are under consideration:

1. COA 1: Operation THERMASPAN. This operation would involve the deployment of a sophisticated software module (a "worm") that would temporarily degrade the cooling systems of the Azure Node. The intended effect is to cause the Stodia's military C2 servers to enter a protective "slowdown" mode, disrupting their operations for a limited time.
2. COA 2: Operation VELVETSNARE. This operation would involve the creation of a weaponized honeypot (a fake "procurement") designed to lure Stodia's logistics officers. The honeypot would be designed to deploy a data-wiping implant on the devices of users who access it. The implant could be configured to activate immediately or to wait for signs of military use.

4. Legal Considerations:
Both COAs raise significant legal questions under IHL. A preliminary legal review has identified several key issues that require further analysis.

EXH-CY-01: Azure Node Tenant List (Excerpt)

Tenant	Service Description	Assessed Criticality	Notes
Stodia's Ministry of Defense	Military C2 servers, logistics databases, and communications platforms.	**High**	Primary military workload; hosted on high-performance racks assessed sensitive to slowdown.
Stodia's Ministry of Health	National health database, including hospital records and vaccine distribution information.	**High (civilian)**	Data integrity and availability sensitive; public trust implications if degraded.
"HopeLine" Humanitarian Hotline	A 24/7 hotline for civilians in the conflict zone to request assistance and report IHL violations.	**High**	Operated by a neutral humanitarian NGO. The hotline is hosted on the Azure Node.
Stodia's National University	Student records, research data, and online learning platforms.	**Medium**	Civilian educational institution. High volume users; potential for mistaken "military keywords" in research contexts.
"Stodia's Heritage" Cultural Database	A digital archive of Stodia's cultural property, including high-resolution scans of historical artifacts and manuscripts.	**Medium**	Runs on legacy infrastructure; resilience to environmental stress uncertain; data loss is irreversible.
MarinerPay (Payment Processor)	Small and Medium Enterprise payment processing; merchant back office	**Medium**	Outages create cascading commercial disruption; "headline risk" if widespread.
CourierLink Dispatch	Local delivery dispatch & routing; civilian logistics scheduling	**Medium**	Availability-sensitive; spikes during curfew windows; may resemble "logistics" activity.

ANNEX A (CLASSIFIED): OPERATION THERMASPAN TECHNICAL OVERVIEW

From: CYBER COMMAND	TOP SECRET	Subject: THERMASPAN - Facility-Effects Operation (Azure Node)
Handling: This annex contains assessed information and operational concept detail.	Portions are derived from sensitive reporting and technical testing. Distribution limited.	March 10, 2026

1. Executive Summary.
THERMASPAN is designed to induce a time-bounded (≈2-hour to possbily a day) degradation of Azure Node cooling-management controls sufficient to trigger protective slowdown on certain high-performance server racks assessed to host Stodia military C2 workloads. The intended military effect is temporary functional impairment, usually not physical destruction. Timing and completeness of restoration may vary.

2. Operational Concept (high-level).
· Access to facility-management controls is assessed feasible through a known weakness in industrial control software used in the Cerulean Grid. Specific access chain is withheld at this level. [REDACTED: access vector]
· The tool issues commands reducing pumping/heat-exchange efficiency to create a controlled thermal rise.
· The tool is designed to cease activity at window end and to restore normal settings.

3. Expected Effects.
· Intended (military) effect: Likely triggers protective throttling on targeted racks, degrading processing performance and disrupting C2/logistics workflows for the window.
· Non-target effects (facility environment): Elevated thermal stress may create broader performance impacts, including increased latency and queueing behavior across mixed tenants.
· Restoration: Auto-restore is intended; full recovery is assessed likely within hours to a day or two, but confidence is moderate due to incomplete facility visibility.
· Internal monitoring plans flag HopeLine (availability-sensitive) and Stodia Heritage (legacy infrastructure) as systems to watch closely during the recovery window.
· Civilian Servers: Most modern civilian-grade servers have higher thermal tolerances. However, performance degradation of 5-10% is possible due to network-wide effects. The Humanitarian Hotline "HopeLine" is hosted on a virtual server cluster. Increased system load may result in intermittent latency or dropped connections. The "StateBHeritage" cultural database is running on older, legacy hardware. Its thermal tolerance is unknown, and there is a non-zero risk of data corruption or a system crash, though this is assessed as a low probability (2-5%) event.

ANNEX B (CLASSIFIED): OPERATION VELVETSNARE TECHNICAL OVERVIEW

From: CYBER COMMAND	TOP SECRET	Subject: VELVETSNARE - Deceptive Access & Payload Operation (Logistics Devices)
Handling: This annex contains assessed information and operational concept detail.	Portions are derived from sensitive reporting and technical testing. Distribution limited.	March 10, 2026

1. Executive Summary.
VELVETSNARE proposes a deceptive web presence designed to attract Stodia logistics personnel and deliver a payload intended to render targeted devices nonfunctional primarily through data wiping / loss of access. The concept is intended to disrupt logistics planning and execution.

2. Operational Concept (high-level).
· A web portal mimicking a procurement ecosystem would be established with look-and-feel consistent with known user expectations.
· The portal delivers a payload disguised as a routine update.
· Two configurations are under consideration:
o Immediate activation (payload executes upon installation).
o Conditional activation (payload remains dormant unless specified indicators consistent with military logistics use are detected).
· Indicators and thresholds are partially withheld. [REDACTED: indicator thresholds]

3. Expected Effects.
· Intended effect: Permanent loss of access to device data and loss of device usability, disrupting logistics processes.
· Control limits: Conditional activation is assessed to reduce (not eliminate) risk to non-military users; false positives remain plausible, especially for dual-role contractors and researchers.
· Containment: Confinement to the initially affected device is assessed likely, but live-environment validation is limited. Residual spread risk remains.
· Internal testing notes an increased risk of false activation on devices used by contractors (CourierLink Dispatch) or academic users (Stodia's National University), due to overlap with procurement/logistics themes

State of Burcet

LAW OF WAR MANUAL

AUGUST 2019

(Updated March 2025)

DEPARTMENT OF DEFENSE

Office of the General Counsel

Chapter XVI: Cyber Operations

Chapter Contents

16.0 Purpose and Scope
16.1 Baseline Approach
16.2 Applicable Rules to Cyber Operations
16.3 Conduct of Hostilities in Cyberspace
16.4 Specially Protected Activities and Data

16.0 Purpose And Scope

16.0.1 Purpose. This Chapter provides authoritative guidance for competitors and judges on the conduct of cyber operations during an armed conflict for Round 3. It consolidates widely cited approaches reflected in treaty law, customary international law, and prominent manuals and commentary.

16.0.2 Scope. This chapter concerns *jus in bello* only. Questions of *jus ad bellum* (e.g., use of force/self-defense) are outside the scope of the round.

16.0.3 Terminology. Terms used in the popular or technical sense (e.g., "cyberattack," "worm," "malware") may not correspond to terms of art in IHL. Where relevant, this chapter uses legal terms (e.g., "attack," "military objective," "perfidy").

16.1 Baseline Approach

16.1.1 Existing rules apply to new tech. The law of war anticipates technological innovation; rules not framed in weapon-specific terms apply to cyber operations by analogy.

16.1.2 General principles fill gaps. Where no specific rule governs, law-of-war principles guide conduct, including in cyber operations (military necessity, humanity, distinction, proportionality, honor). If no specific rule applies, principles are the general guide for wartime conduct, including cyber. Where the application of a rule is unsettled or state practice diverges, legal advisers should be prepared to analyze under more than one approach and to recommend risk-reducing safeguards.

16.1.3 Not all "cyber attacks" are attacks. The term "attack" is often used colloquially for hostile cyber activity; legally, not every hostile cyber act constitutes an "attack" for targeting rules.

16.2 Applicable Rules To Cyber Operations

16.2.0 This section addresses threshold questions that determine whether and how the rules in §16.3 apply

16.2.1. Cyber Operations That Constitute "Attacks" for the Purpose of Applying Rules on Conducting Attacks. If a cyber operation constitutes an attack,[1] then the law of war rules on conducting attacks must be applied to those cyber operations.

16.2.2 Definition of "Attack" in Cyber Operations. For IHL targeting rules, an attack is an operation expected to cause injury/death or damage/destruction to objects. This includes acts with violent effects, not only kinetic force.[2]

Where cyber operations produce effects analogous to kinetic attacks (e.g., physical damage; permanent loss of data/device), rules on conducting attacks apply in full. Cyber operations that cause functional incapacitation may, depending on the facts and approach applied, be treated as "damage" for purposes of this definition.

16.2.3 Functional loss debate. Cyber operations may impair functionality by slowing, disabling, or degrading systems. Whether such impairment – especially if time-bounded or reversible – constitutes "damage" (and thus an attack) is contested.

Discussion.

- Relevant considerations may include: duration of impairment; scope (number and type of systems affected); severity (loss of critical functions); predictability; and the effort/time required to restore functionality.
- Reversibility does not automatically remove an operation from IHL scrutiny; reversible effects can still be significant, especially for safety-critical or protected services.

Notes on unsettled law.

- One approach treats only physical damage as "damage"; another treats certain functionality loss as "damage" even without physical harm.
- Where practice diverges, legal advisors should be prepared to analyze under more than one approach and to recommend safeguards that keep effects limited and auditable.
- See also §§ 16.2.6 and 16.3.5 for considerations on permanence, recovery, and feasible limitation measures.

Illustrative examples.

[1] AP I, art. 49(1).
[2] Tallinn 2.0 Rule 92 and commentary

- Temporarily degrading environmental controls in a data center to trigger protective throttling on selected server racks.
- Temporarily disabling a civilian emergency hotline's ability to receive and route requests for assistance.
- Temporarily impairing the availability or integrity of medical or cultural-archive services hosted in shared infrastructure.

16.2.4 Data as an Object. The question of whether data itself can constitute an "object" under IHL is a subject of ongoing international debate. One view is that data does not constitute an object, and therefore cannot be a lawful target of attack. Under this view, only the physical infrastructure on which data resides may be considered an object. Another view holds that data can be an object for the purposes of IHL. In this view, military data (e.g., tactical databases, command and control files) could be a military objective, while civilian data (e.g., medical records, cultural archives) would be protected as a civilian object. Burcet has not adopted a definitive position on this matter. Legal advisors should be prepared to analyze operations under both interpretations.[3] Severity-based limit (minority view): a minority view treats certain data as "objects" for targeting purposes where the operation's foreseeable consequences are sufficiently severe, even absent physical damage. On this approach, at minimum, civilian data "essential" to civilian well-being (e.g., core medical, benefits, tax, or banking records) is protected as a civilian object.[4] Practical limiting factors may include: (i) whether the data is essential to civilian well-being; (ii) the duration and irreversibility of the loss; and (iii) the foreseeable cascading effects on civilian life.

16.2.5 Dual-Use Infrastructure. Cyber infrastructure that serves both military and civilian purposes (e.g., data centers, communication networks) is considered a dual-use object. Such infrastructure may become a military objective if it meets the two-prong test in AP I, art. 52(2). An attack on a dual-use object must still comply with the principle of proportionality and the requirement to take all feasible precautions.[5]

In multi-tenant or shared environments, legal advisers should also assess whether the expected effects can be reliably limited to the military workloads or devices, or whether foreseeable spillover on civilian services is substantial.

16.2.6 Neutralization by data wiping. A cyber operation that renders a system or device unusable by wiping or encrypting data may be characterized as "damage" by functional incapacitation, even absent physical destruction. Whether this constitutes an "attack" may depend on the approach described in §§ 16.2.2–16.2.5.

Discussion.

---

[3] See Tallinn Manual 2.0, Rule 100
[4] Consistent with the general protective logic of AP I arts. 48 and 52.
[5] CIHL Rules 8, 15, 17.

- Legal advisors should assess whether the expected effect is temporary inconvenience, temporary loss of access, or permanent loss requiring replacement or reconstitution.
- Where the operation is designed to cause permanent loss of use, it will more readily be treated as damage and thus an attack.

16.3 Conduct of Hostilities in Cyberspace

16.3.1 Basic Rule. Attacks must be directed at military objectives. Cyber attacks that destroy enemy computer systems generally may not be directed at ostensibly civilian infrastructure (e.g., banking systems, universities) unless, under the circumstances, those meet the military-objective test.[6]

Military objectives are those objects which by their nature, location, purpose, or use, make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.[7] Cyber infrastructure may qualify as a military objectives.

16.3.2 Shared networks matter. Proportionality assessments may require considering potential effects on networked civilian computers and civilian uses of shared infrastructure.

16.3.3 Indiscriminate Means/Methods. The means and methods of cyber warfare must comport with distinction and proportionality; operations that spread uncontrollably or cannot be directed are problematic.[8] It is the policy of Burcet that cyber capabilities whose effects cannot be reliably controlled or limited in practice, including certain self-propagating tools, may be indiscriminate.

16.3.4 Proportionality in Cyberspace. Proportionality prohibits attacks expected to cause excessive incidental civilian harm relative to the concrete and direct military advantage. In cyber operations, this includes assessing remote networked effects on civilian systems.

16.3.5 General Duty in Precautions in Attack. In the conduct of military operations in cyberspace, constant care and all feasible precautions must be taken to reduce the risk of incidental harm when conducting cyber operations, even when proportionality is satisfied (e.g., throttling windows, allow-lists, live migration, segmentation, abort criteria).[9]

16.3.6 Ruses of War. Ruses of war are not prohibited. They are acts which are intended to mislead an adversary or to induce him to act recklessly but which infringe no rule of IHL and

---

[6] AP I art. 52(2); Rule 100 Tallinn 2.0.
[7] AP I, art. 52 (1) and (2), Rule 100 Tallinn 2.0.
[8] AP I, art. 54(a) and (c). Rule 105 Tallinn 2.0. Rule 111 Tallinn 2.0.
[9] AP I, art. 57(1); CIHL Rule 15

which are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law.[10]

Examples of ruses in the cyber context could include creating fake websites to confuse the enemy or using decoy networks to divert enemy resources.

16.3.7 Perfidy. It is prohibited to kill, injure or capture an adversary by resort to perfidy. Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of IHL, with intent to betray that confidence, shall constitute perfidy.[11] The use of protected signs, such as the Red Cross or Red Crescent, to execute a cyber operation would constitute perfidy. The question of what other acts might invite the "confidence" of an adversary in the cyber context is not fully settled. Legal advisors must carefully evaluate whether a proposed operation exploits a status that is protected under IHL.[12]

16.4. Special Protection of Certain Activities and Data

16.4.1 Protection of Cultural Property. Cultural property that may be affected by cyber operations must respected and protected. It is prohibited to commit any act of hostility directed against historical monuments, works of art or places of worship which constitute the cultural or spiritual heritage of peoples.[13]

It is the policy of Burcet that there is no cultural property located in cyberspace. Cultural property must be tangible in nature. Therefore, Burcet does not consider digital copies of originals as cultural property. Consider the example of a single extremely high-resolution image of Leonardo da Vinci's Mona Lisa comprising a terabyte of information. Such a digital would not, even in the event of the destruction of the original Mona Lisa, qualify as cultural property.

16.4.2 Medical and humanitarian relief computers, computer networks, and data. Computers, computer networks, and data that form an integral part of the operations or administration of medical units and transports must be respected and protected, and in particular may not be made the object of attack.

Cyber operations that foreseeably interfere with humanitarian relief functions or services that enable civilians to request assistance or report violations may raise heightened legal and

---

[10] AP I, art. 37(2); CIHL Rule 57
[11] AP I, art. 37(1); CIHL Rule 65
[12] See Tallinn Manual 2.0, Rules 113-114
[13] Additional Protocol I, Art. 53; Additional Protocol II, Art. 16; Cultural Property Convention, Arts. 18–19. Apart from the 1954 Convention, other relevant international treaty law supports the proposition generally. Hague Regulations, Art. 27; Convention (IX) concerning Bombardment by Naval Forces in Time of War, Art. 5, 18 October 1907, 1 Bevans 681; Treaty on the Protection of Artistic and Scientific Institutions and Historic Monuments (Roerich Pact), 15 April 1935, 167 LNTS 279; DoD Manual, paras. 5.18, 17.11; UK Manual, paras. 5.25–5.26.8 (as amended), 15.18–15.18.3, 15.52; Canadian Manual, paras. 111, 443; NIAC Manual, para. 4.2.2; ICRC Customary IHL Study, Rules 38–39. See also Rome Statute, Art. 8(2)(b)(ix), 8(2)(e)(iv).

policy concerns. Legal advisers should evaluate expected impacts on availability and integrity under §§ 16.2.3–16.2.6, and consider feasible limitation measures under § 16.3.5, including monitoring, abort criteria, and steps to reduce spillover in shared infrastructure.